NOVAFCSH
FACULDADE DE CIÊNCIAS SOCIAIS E HUMANAS
UNIVERSIDADE NOVA DE LISBOA

NOVA IMS Information Management School

Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação

Marina Romano Aleixo

Dissertação de Mestrado em Gestão e Curadoria da Informação

Nota: Marina Romano Aleixo, Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação, 2020

Setembro 2020

Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação

Marina Romano Aleixo

Dissertação de Mestrado em Gestão e Curadoria da Informação

Orientador Professor Doutor José Borbinha

Coorientação Professora Doutora Paula Alexandra Ochôa de Carvalho Telo

Setembro 2020

Tese apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão e Curadoria da informação, realizada sob a orientação científica do Professor Doutor José Borbinha e da Professora Doutora Paula Alexandra Ochôa de Carvalho Telo

AGRADECIMENTOS

A todos aqueles que contribuíram, direta ou indiretamente, para o desenvolvimento deste trabalho, quero agradecer profundamente.

Agradeço, especialmente ao meu orientador Professor Doutor José Borbinha por todo conhecimento, tempo e paciência que me há dispensado. Ademais, quero agradecer também à Professora Doutora Paula Ochôa que também me acompanhou e incentivou na realização deste trabalho. Sem o empenho, a dedicação e o apoio de ambos na busca de soluções para minhas inúmeras questões seria impossível finalizá-lo.

Agradeço também a todo o corpo docente da FCSH e da NOVA IMS que muito contribuíram para meu desenvolvimento académico, pessoal e profissional.

À minha família, em especial à minha mãe e irmã, por todo apoio e compreensão e por emprestar seu conhecimento, ombros e ouvidos e me ajudarem a superar meus obstáculos.

E por fim, quero agradecer imensamente aos meus amigos, mas, ainda mais, a duas das melhores pessoas que conheci nesta longa jornada: Gislane Costa e Maria Fernandes. Obrigada pelas inúmeras horas de *brainstorming*, risadas e apoio que, tenho certeza, sem estas não conseguiria prosseguir.

Lista de Figuras

Lista de Tabelas

Sumário

Alinhamento das práticas da gestão e curadoria da informação com as da segurança da informação

Marina Romano Aleixo

Resumo

A evolução da tecnologia proporcionou uma mudança do cenário na sociedade da informação. Ela possibilitou o surgimento de fenómenos como o *big data*, no qual o crescimento exponencial de informação atinge a sociedade a cada minuto. Com isso, garantir a confidencialidade, integridade e disponibilidade da informação tornou-se uma tarefa fundamental. As áreas da segurança da informação e gestão e curadoria da informação têm como objetivo garantir isso aos interessados, sendo, no entanto ainda pouco estudada a extensão das suas sobreposições ou complementaridades mútuas. Este trabalho propõe uma contribuição para essa questão, apresentando uma proposta de alinhamento entre os processos e práticas da segurança da informação e da gestão e curadoria da informação, de maneira a garantir melhor eficácia e eficiência em organizações nas quais essas áreas de interesse coexistam. Para tal, utilizou-se o método de pesquisa bibliográfica, primeiro para elucidação e explanação dos principais conceitos dessas áreas e respetivos sistemas de gestão, e de seguida para a identificação de estudos exploratórios de análises de tendências e exemplos de investigação. Conclui-se que é possível a sinergia dos processos, e que uma aplicação conjunta dos dois sistemas de gestão melhoraria a eficácia e a eficiência numa organização.

Palavras-chave: Gestão e curadoria da informação. Segurança da informação. Alinhamento. Processos.

Alignment of information management and curation and information security practices

Marina Romano Aleixo

Abstract

The evolution of technology had changed the information society. It enabled the appearance of a phenomena know as big data, which deals with the exponential growth of information that reaches society every minute. Thus, ensuring the confidentiality, integrity, and availability of information has become a fundamental task. The domains of information security and information management and curation also have the objective to guarantee this to the stakeholders. This dissertation aims to present a contribution to this matter, a proposition of alignment between the information security and information management and curation processes and practices, as a means to guarantee better effectiveness and efficiency in organizations in which these areas of interest coexist. For this purpose, bibliographic research method was used to elucidate and explain the main concepts of these areas and their respective management system, and to identify exploratory studies of trend analysis and research examples. In conclusion it is possible to have a synergy of processes and that a joint application of both management systems would improve its effectiveness and efficiency in an organizations.

Keywords: Information management and curation. Information security. Alignment. Process.

1. Introdução

A evolução tecnológica apresenta novos paradigmas à sociedade, a qual saiu de uma era industrial, para entrar na era do conhecimento. Nesta nova era a sociedade gera, consome, distribui e explora a informação de maneira rápida e abundante (Burke, 2003; Castells, 1999; Werthein, 2000). Desta forma, a informação torna-se o foco principal dessa sociedade, de maneira que todos os processos são embasados e dependentes dela, além de que devido ao desenvolvimento de novas tecnologias o seu volume se expande exponencialmente, como observado no fenómeno do *Big data* (De Mauro et al., 2014; Li & Zhu, 2015). De Mauro et al. (2014), define *Big data* como o alto volume, velocidade e variedade dos ativos informacionais e, para que possam ter valor, necessitam de tecnologias e métodos analíticos apropriados. Novos desafios e questões são apresentados por este evento, como por exemplo: Como é possível garantir confidencialidade e integridade dos dados? Como fazer a sua gestão de maneira a permitir a disponibilidade dos recursos?

Uma das respostas a essas questões é trazida pela gestão e curadoria da informação (GCI). Esta é uma nova área interdisciplinar que visa gerir a informação desde o início de seu ciclo de vida, garantindo a sustentabilidade da informação, o seu tratamento e agregação de valor, mediante o uso pretendido e as necessidades dos interessados (*stakeholders*). Trata-se de uma área interdisciplinar, juntando as perspetivas da ciência da informação, gestão da informação (GI) e curadoria da informação (CI) que pretende desenvolver novos perfis profissionais, mediante as necessidades do mercado (Henriques, 2017; Ochôa, 2017).

Outra área que vem incidir sobre essas questões é a da segurança da informação (SI), pois é o campo de estudo que vem influir sobre a preservação do valor dos recursos de maneira a assegurar a disponibilidade, a integridade e a confidencialidade. É uma área em constante desenvolvimento e que afeta a sociedade em muitos setores. Segundo pesquisa realizada pela BBC (2019), só no primeiro semestre de 2019 mais de metade das empresas no Reino Unido sofreram ataques de cibersegurança; Newman (2019) aponta que nos Estados Unidos, mais de 100 mil pessoas foram afetadas num único ataque ao departamento americano *US Customs and Border Protection* (Serviço de Alfândegas e Proteção das Fronteiras dos Estados Unidos) devido ao roubo de informações e Aitken (2018) estima na sua pesquisa realizada em 2018, uma projeção de gastos mundial de mais de US$124 biliões em 2019 em questões relativas à SI.

Dessa forma, a GCI e a SI devem ser estudadas de forma correlacionada, dado que ambas visam condições ideais de acesso, integridade e disponibilização dos dados, garantindo que os mesmos não estejam corrompidos, sejam confiáveis e possam atender à demanda informacional da sociedade. Isto corrobora a pertinência dessa pesquisa, devido a necessidade de criação, distribuição, seleção, exploração e disseminação da informação de forma precisa e com alta qualidade.

Neste contexto, este estudo formula a seguinte questão de investigação: será possível desenvolver um alinhamento entre os processos de GCI com os da SI de maneira a melhorar a eficiência e eficácia desses processos nas organizações onde tenham de coexistir?

Para responder a esta questão, esta pesquisa utilizar-se-á do método de pesquisa bibliográfica, para elucidação e explanação dos principais conceitos dessas áreas, além de estudos exploratórios de análises de tendências e exemplos de investigação para a comparação e desenvolvimento de uma proposta de alinhamento entre os processos de ambas áreas.

Com isto, este trabalho tem como objetivo geral: identificar nos processos e objetivos de, por um lado, a GCI e, pelo outro, da SI, oportunidades de sinergias que possam levar a uma melhor eficiência e eficácia desses processos nas organizações onde tenham de coexistir. Ademais tem também como objetivos específicos:

- Analisar de que modo diferem ou se assemelham os objetivos por um lado da GCI e, por outro, os da SI;
- Identificar em que modo diferem ou se assemelham os princípios, processos, métodos e técnicas por um lado da GCI e, por outro, os da SI;
- Investigar e apontar como os objetivos, princípios e práticas de GCI e SI podem ser formulados, entendidos e praticados de forma alinhada entre si; e
- Contribuir para o desenvolvimento e melhoria das práticas da GCI aplicadas à SI através de uma proposta de alinhamento.

Este estudo está estruturado em quatro partes principais: 1ª) os capítulos 2, 3 e 4 – Informação, GCI e SI, nos quais se encontram a elucidação dos principais termos da pesquisa e a base teórica da mesma; 2ª) os capítulos 5 e 6 – Modelo concetual e Metodologia, que apresentam o desenho da pesquisa e a metodologia utilizada para o desenvolvimento deste estudo; 3ª) os capítulos 7 e 8 - Análise comparativa dos processos

e Proposta de alinhamento, nos quais serão apontados as principais semelhanças e diferenças dos processos, além de uma proposta de alinhamento e a discussão pertinente; e a 4ª parte que é referente à conclusão da pesquisa e considerações finais.

Um dos principais resultados da pesquisa é relativo à melhoria da eficácia e eficiência dos processos quando melhor estruturados e da sua aplicabilidade nas organizações. Os processos das duas áreas são possíveis de serem alinhados e conferem maior granularidade entre si, não perdendo a sua característica holística.

2. Informação como ativo de valor e as suas vulnerabilidades

O conceito de informação tem sido definido de diversas formas ao longo dos tempos. Uma das primeiras definições de informação foi discutida no artigo *A mathematical theory of communication*, no qual Shannon (1948) apresenta a teoria da informação e os aspetos sobre a transmissão da informação através de canais. A definição apresentada por Shannon (1948), apesar de atual em muitas áreas como Engenharia em geral e Física, possuem diferentes mudanças e significados quando vinculadas às outras áreas de estudo e teorias nas quais estas estão inseridas conforme apontam Capurro e Hjørland (2003).

Muitas teorias vinculam a definição de informação às de dados e conhecimento (Zins, 2007), como a KBI (*Knowledge-Based Theory of Information* - Kettinger & Li, 2010) e DIKW (*Data, Information, Knowledge, Wisdom* - Baskarada & Koronios, 2013; Liew, 2013). Contudo, uma das teorias mais discutidas e aceites na área da ciência da informação é a teoria da hierarquia dos termos dados - informação - conhecimento (Benjamin Martz Jr. & Shepherd, 2003; Davenport & Grover, 2001). Nesta teoria, dados são definidos como "a codified and communicable symbolic representation of entities, properties and their states. They have content (representation) and form (record) that allow storage, retrieval, transfer, aggregation, and analysis"[1] (Lillrank, 2003, p. 693). A informação, entretanto, é definida como os dados acrescido de contexto e significado (Davenport & Grover, 2001; Lillrank, 2003).

Davenport e Grover (2001) designam conhecimento como a parte que possui maior contribuição humana e tem maior valor, além de ser o que possui maior relevância às tomadas de decisões e o que pode ser mais afetado dependendo do contexto ou de uma situação específica. Os autores ainda apontam que entre os dados, informação e conhecimento, este último é o mais difícil de gerir, pois este origina-se na mente humana e estão sempre conectados às pessoas que possuem este conhecimento, pois elas têm a habilidade de integrar a informação com o contexto, com a sua experiência e julgamento e enquadrá-los nas situações.

Dessa forma, a informação é dependente dos dados, significado e contexto, para existir, já o conhecimento depende da informação e da capacidade humana de integração

[1] "uma representação simbólica comunicável e codificada de entidades, propriedades e seus estados. Eles possuem conteúdo (representação) e forma (arquivo) que permite seu armazenamento, recuperação, transferência, agregação e análise" (Lillrank, 2003, p. 693 tradução nossa).

a outros contextos e informações. Capurro e Hjørland (2003), citam as teorias de Nonaka e Takeuchi (1995), Polanyi (1966) e Krogh et al. (2000), que diferenciam o conhecimento tácito (implícito) do conhecimento explícito (informação representada), no sentido em que somente o conhecimento explícito, pode ser gerido, dado que o conhecimento tácito está somente na mente humana.

2.1 Ativos informacionais e valor da informação

Nas organizações, as informações estão presentes em todos os departamentos. Desde procedimentos, normas, processos, instruções, *softwares*, relatórios, planos, etc. Assim, devido ao seu valor para a organização, as informações podem ser consideradas ativos (Davenport & Grover, 2001). Esses ativos informacionais são intangíveis e muitas vezes só possuem registo em transcrições físicas (Sajko et al., 2006, p. 265), os quais podem ser geridos (Capurro & Hjørland, 2003).

Numa entrevista para a Forbes em 2012, Douglas Laney destaca a importância de avaliar o valor da informação numa organização (Laney, 2012). A realização deste processo é crucial à organização, devido:

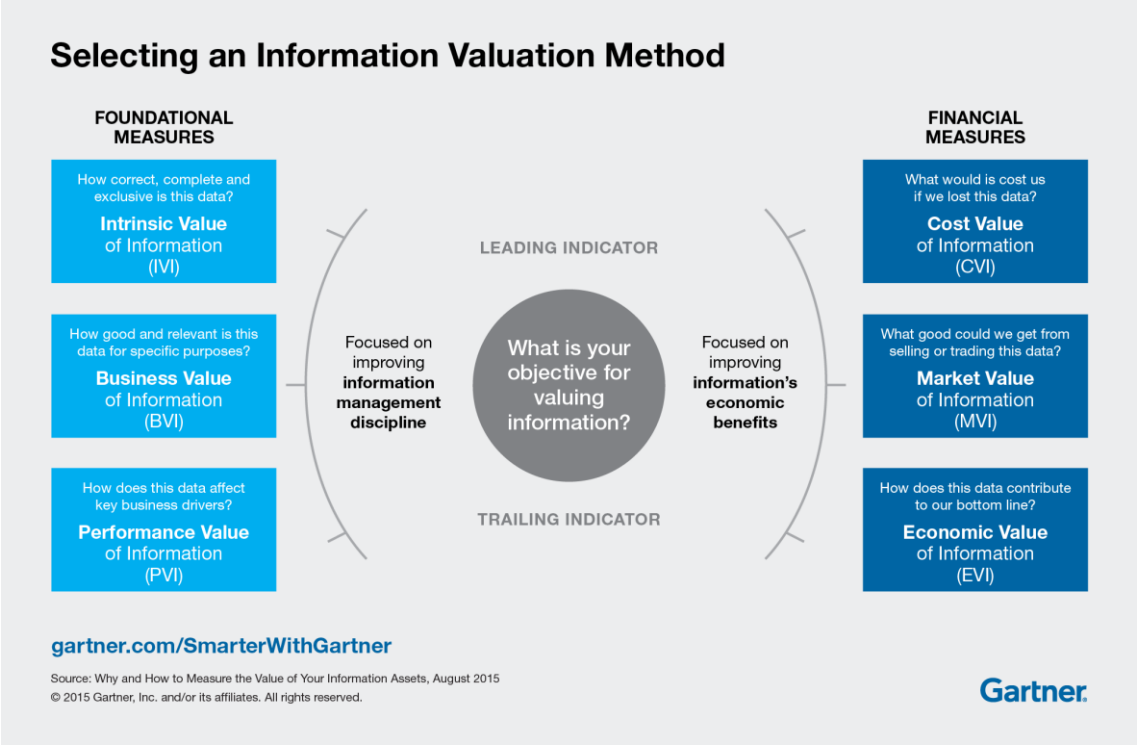
- à melhoria da gestão, dado que é necessário a realização de um mapeamento das informações disponíveis para poder entendê-las e melhor geri-las;
- ao entendimento do verdadeiro valor do retorno de investimento que as informações proporcionam à organização;
- à aplicação de procedimentos para proteger as informações;
- à influência no valor da organização;
- à avaliação dos riscos contratuais; e
- à negociação de informações, como venda de dados, entre outros.

Por outras palavras, para avaliar o valor da informação, deve-se considerar o significado que esta possui para o negócio (tanto em relação aos potenciais lucros, à sua utilidade, ao seu custo e à sua precisão) (Sajko et al., 2006). Contudo, para essa avaliação, deve atentar-se a todas às formas disponíveis da informação, ou seja, tanto a informação tangível (como processos, normas, imagens, etc.), quanto a informação intangível (como ideias, marcas, conceitos) (ISO/IEC, 2013b, p. vi).

Sajko et al. (2006) apontam que a intangibilidade da informação dificulta a ação de determinar o seu valor e que esta é uma tarefa pouco precisa. Ademais, diversos fatores impactam esta mensuração, tais como o peso de evidência da informação (Wang & Wong, 2003), o seu capital social (Yang & Farn, 2009), o seu significado (Lillrank, 2003) e a sua complexidade (Gu & Wang, 2005). Gouveia (2016, p. 6) complementa que o valor da informação advém das características que a própria informação possui e, "se, por qualquer motivo, a informação altera alguma das suas caraterísticas, o valor da informação também é alterado".

O Gartner *Information Valuation Method* (*Why and How to Value Your Information as an Asset*, 2015) propõe três métricas fundamentais e três métricas financeiras (figura 1), de forma a se avaliar e permitir melhorar a GI e o desempenho do negócio.

Figura 1 - *Método Gartner de avaliação de valor da informação.*



Fonte: Gartner (*Why and How to Value Your Information as an Asset*, 2015).

Segundo este, devem-se aplicar as métricas fundamentais de avaliação da informação para priorizar e melhorar a disciplina de GI. Estas métricas são baseadas no:

- Valor Intrínseco da Informação (IVI – *Intrinsic Value of Information*): Avalia quão corretos, completos e exclusivos são os dados;
- Valor Empresarial da Informação (BVI – *Business Value of Information*): Avalia quão bons e relevantes são os dados relativamente a propósitos específicos; e
- Valor de Desempenho da Informação (PVI – *Performance Value of Information*): Avalia o quanto esses dados podem afetar os principais indicadores de negócio.

O modelo ainda orienta para o dever de aplicar as métricas financeiras de avaliação da informação para acelerar e melhorar o benefício económico da informação. Estas métricas são baseadas no:

- Valor de Custo da Informação (CVI – *Cost Value of Information*): Avalia o quanto custaria a perda dos dados para o negócio;
- Valor de Mercado da Informação (MVI – *Market Value of Information*): Avalia o quanto a empresa lucraria por vender ou negociar os dados; e
- Valor Económico da Informação (EVI – *Economic Value of Information*): Avalia o quanto os dados contribuem para o resultado dos negócios.

Métricas como a IVI e CVI são consideradas como indicadores principais (*leading indicators*), ou seja, ajudam a prever a mudança do cenário económico e de negócios (J. Chen, 2018). Outras medidas, como PVI e a EVI podem ser consideradas como indicadores secundários (*trailing indicators*), isto é, indicadores que dão suporte aos indicadores principais de maneira ajudar à tomada de decisão, através da análise de informações recolhidas depois da mudança do cenário económico (Chappelow, 2020).

Em outras palavras, a avaliação da informação deve ser realizada de maneira a desenvolver indicadores que suportem a gestão, permitindo melhor análise dos negócios, de forma a aprimorar os resultados. Contudo, nota-se que essa valoração da informação depende de diversos fatores e dado que cada organização trabalha de maneira singular e possui características únicas, esta tarefa torna-se peculiar e deve ser adaptada ao contexto da organização e às suas necessidades.

2.2 Classificação da informação o segundo seu acesso

Um exemplo de referência para níveis de classificação da informação é o que foi desenvolvido pela Associação Brasileira de Normas Técnicas na norma *NBR 16167:2013 Segurança da informação: diretrizes para classificação, rotulação e tratamento da informação* (ABNT, 2016). Esta sugere quatro níveis que devem ser definidos pela organização, considerando aspetos como o "valor da informação, os requisitos legais, a sensibilidade, a criticidade, o prazo de validade (ou vida útil), a necessidade de compartilhamento e restrição, a análise de riscos e os impactos para o negócio" (Winter & Botelho, 2014):

- Nível 1 – Informação pública: informações que podem ser divulgadas de forma pública, tanto ao público interno e externo da organização;
- Nível 2 – Informação de uso interno: informações que podem ser divulgadas somente para o público interno da organização;
- Nível 3 – Informação restrita: informações que só podem ser divulgadas a certos públicos, cargos, ou áreas dentro da organização; e
- Nível 4 – Informação confidencial: informações de caráter sensível que requerem um nível especial de tratamento e não podem ser divulgadas de forma não autorizadas.

É importante referir que, apesar desta norma sugerir estes níveis de classificação, a classificação dos ativos informacionais deve ser realizada estabelecendo-se diferentes níveis e critérios, tais como, a importância do ativo informacional, o seu sigilo, o seu valor, a sua criticidade, os seus requisitos legais relevantes, entre outros (Campos, 2014; Dantas, 2011; ISO/IEC, 2013a; Whitman & Mattord, 2016). Cada proposta de classificação é única e é dependente dos objetivos da organização, seus processos, suas normas, seus procedimentos, etc. Considera-se, no entanto, este sistema de classificação representativo do que é geralmente considerado para o efeito na grande maioria das empresas e administrações públicas, pelo que o mesmo é aqui apontado apenas como um de muitos outros exemplos que se poderiam apontar.

2.3 Vulnerabilidades da informação

A informação, assim como outros ativos numa organização, possui naturalmente vulnerabilidades. As vulnerabilidades são "fraquezas que podem ser exploradas por uma

ou mais ameaças" (ISO/IEC, 2018, p. 11). Essas são inerentes e intrínsecas ao ativo e podem vir a ser exploradas intencionalmente ou não (Campos, 2014; ISO/IEC, 2018; Whitman & Mattord, 2016). Dantas (2011, p. 24) aponta que essas vulnerabilidades "por si só, elas não provocam incidentes, pois são elementos passivos, necessitando para tanto de um agente causador ou de condição favorável [ameaças]".

Em relação à identificação dos tipos de vulnerabilidades, Campos (2014), infere que é possível elencá-las por áreas, como:

- Tecnológicas: partes tecnológicas que possam vir a ser exploradas de maneira a obter informações, como, por exemplo, portas USB, CDs, internet, redes, cabos de redes, aparelhos de fax, sistemas de informação;
- Pessoas: divulgação indevida por parte de pessoas, seja acidentalmente ou pela utilização de técnicas como a engenharia social;
- Processos: processos e procedimentos que não são claramente definidos e/ou não foram totalmente esclarecidos, de maneira a gerar divulgação da informação; e
- Ambientes: ambientes estão sujeitos a sinistros, tanto por forças naturais (como terremotos, cheias ou outras catástrofes), quanto por invasão indevida ou ação criminosa.

Outros autores como Whitman e Mattord (2016) e Dantas (2011, p. 26), expõem outras maneiras de classificação das vulnerabilidades, como: "naturais, organizacionais, físicas, de *hardware*, de *software*, nos meios de armazenamento, humanas e nas comunicações"; além das suas possíveis ameaças, por exemplo, comprometimento da propriedade intelectual, espionagem, forças da natureza, extorsão de informação, sabotagem, ataques de *softwares*, falhas técnicas de *softwares* e *hardwares*, roubo, entre outros (Whitman & Mattord, 2016).

Essas categorizações devem ser realizadas considerando os objetivos e necessidades da organização e observando que essas vulnerabilidades existem e não podem ser extintas, contudo é possível minimizar os riscos, através da aplicação de processos da SI. Fazer a listagem das vulnerabilidades depende muito do conhecimento e experiência da pessoa envolvida na tarefa, mas é desta lista que sairão as abordagens necessárias para a proteção dos ativos informacionais (Whitman & Mattord, 2016).

2.4 Classificação da informação segundo a sua vulnerabilidade

É importante poder classificar os ativos informacionais segundo as suas vulnerabilidades, de forma a melhor utilizá-los, geri-los e mantê-los seguros. Assim, é possível realizar a classificação dos ativos informacionais, de maneira que as ações necessárias à sua segurança sejam implementadas.

Segundo a norma ISO/IEC 27002 (ISO/IEC, 2013b), o objetivo de classificar a informação é assegurar que ela receba um nível adequado de proteção. Para isso, a informação deve ser classificada considerando o seu valor à organização, os seus requisitos legais, a sua sensibilidade e a sua criticidade (ISO/IEC, 2013b). Ademais, ela deve ser rotulada e passar por um tratamento que será definido de acordo com a classificação da informação. A classificação da informação, segundo Whitman e Mattord (2016, p. 241), determina o nível de informação que cada colaborador está autorizado a ver consoante o que ele precisa saber.

Gouveia (2016) aponta que esse processo de classificação deve ser dividido em quatro etapas, iniciando-se com a identificação do ativo de informação a ser inventariado, além do seu uso e os responsáveis por eles. A segunda etapa consiste na classificação da informação, apontando os seus níveis. A terceira etapa é referente à rotulagem da informação, que deve ser realizada de maneira clara e visível, de forma que o responsável pela informação e todos os envolvidos no seu uso compreendam o nível de informação que estão a lidar. A quarta e última etapa é relativa à manipulação e manuseio dos ativos, ou seja, a descrição sobre processos de segurança quanto ao armazenamento, transmissão, novas formas de classificação (caso necessário) e descarte das informações.

Estes mesmos passos podem ser encontrados no anexo A.8.2 da norma ISO/IEC 27001, no qual apresenta controlos para a classificação da informação (classificação da informação, rotulagem da informação e manuseio dos ativos), apesar de não propor níveis para tal.

Em suma, compreende-se que a informação, como qualquer outro ativo de uma organização, deve ser reconhecida, analisada, listada e classificada. Deve-se identificar as vulnerabilidades que a compõe e a sua importância para a organização, de maneira a poder classificá-las e, assim, ser utilizada da melhor forma nos processos de GCI, assim como para que os procedimentos de SI possam ser aplicados, como serão apresentados nos capítulos a seguir.

3. Gestão e curadoria da informação

A GCI é uma área interdisciplinar que vem suprir lacunas existentes no mercado de trabalho e académico (Reyes et al., 2017). Ela desenvolveu-se a partir das necessidades do novo cenário mundial e devido ao avanço de novas qualificações requeridas para atender essa demanda, baseando-se em novos perfis e competências necessárias para tal (Pinto & Ochôa, 2006; Barata & Ochôa, 2015; Ochôa, 2017; Reyes et al., 2017; Silva et al., 2019). Estas competências podem ser descritas como "conjunto de conhecimentos, atitudes e habilidades necessárias para se ter uma parte ativa nos ambientes digitais e colher os benefícios das tecnologias no quotidiano" (Ochôa & Pinto, 2017, p. 393).

Para o desenvolvimento de uma disciplina aplicada, como é o caso da GCI, Higgins (2018) aponta que o objeto de pesquisa concentra-se nas competências relevantes para o emprego. Ademais, estas disciplinas aplicadas situam-se num ciclo de *feedback* entre a academia e o mercado, no qual a academia desenvolve a teoria, a pesquisa e o currículo e o mercado desenvolve a prática, a agenda social e o conhecimento, voltando assim, à academia novamente. E, dessa forma, este ciclo garante que a disciplina esteja alinhada tanto com a academia, mantendo o seu rigor intelectual, quanto com o mercado de trabalho.

Para melhor compreender a necessidade do avanço da área da GCI, em relação ao mercado, observa-se a imprescindibilidade do desenvolvimento de novas habilidades e competências para enfrentar os novos desafios. Um exemplo é a iniciativa do mercado único digital proposto pela Comissão Europeia devido ao avanço das tecnologias da informação e comunicação (TIC). Essa iniciativa visa que a União Europeia obtenha melhor aproveitamento da nova era digital e, com isso, apreende quais domínios necessitam maiores medidas (EUR-lex, 2020; Maciejewski & Gouardères, 2019).

Outro exemplo da necessidade do desenvolvimento das competências e habilidades pode ser encontrado no estudo que foi desenvolvido pela Comissão Europeia, o Quadro Europeu de Competência Digital para Cidadãos (Digcomp). Este estudo é uma ferramenta que permite aos Estados da União Europeia elaborar iniciativas de planeamento estratégico e desenvolvimento de competências digitais, como por exemplo de literacia de dados e informação, comunicação e colaboração, criação de conteúdo digital, segurança digital e solução de problemas (Carretero Gomez et al., 2017).

Consoante este novo paradigma, a academia portuguesa tenta proporcionar aos estudantes meios para se adequarem ao mercado e desenvolverem as suas competências. Esta é a proposta do Mestrado em GCI, uma parceria das Faculdade de Ciências Sociais e Humanas (FCSH) e da *Information Management School* (IMS) da Universidade Nova de Lisboa (Henriques, 2017). A sua primeira edição foi em 2017-2018 e possui como estrutura curricular as seguintes unidades curriculares obrigatórias e optativas (tabela 1):

Tabela 1 - *Unidades curriculares do Mestrado em GCI.*

Obrigatórias	**Área de estudo**
Análise de Social Media	Comunicação e Marketing
Curadoria da informação: aquisição e organização	CI
Curadoria da informação: preservação e recuperação da informação	CI
Fundamentos da Ciência da Informação	Ciência da informação
Gestão dos sistemas de informação	GI
Gestão e Comportamento Organizacional	GI
Informação e Sociedade	Ciência da informação
Marketing e comunicação da informação	Comunicação e Marketing
Seminário de Investigação e Métodos em Ciências da Informação e Gestão da Informação	Ciência da Informação e GI

Optativas	**Área de estudo**
Análise de Dados	GI e CI
Auditorias da informação	GI
Avaliação da informação	GI e CI

Avaliação de desempenho e sustentabilidade dos serviços de informação	Ciência da informação
Comércio eletrónico	GI
Direito e Ética da Informação	Ciência da informação
Empreendedorismo Cultural	GI e Curadoria da informação
Estudos Métricos da Informação Científica	Ciência da informação
Gestão de Projetos	GI
Introdução aos Linked Data	CI
Marketing Digital	Comunicação e Marketing
Metadados para Objetos Digitais	GI e CI
Políticas Públicas e Governança da Informação	GI e CI

Fonte: Adaptado de Mestrado em Gestão e Curadoria de Informação | NOVA Guia de Cursos (2020).

Nota-se, através da estrutura curricular, a característica interdisciplinar do curso. E, segundo Henriques (2017, p. 44), esta interdisciplinaridade advém "das áreas das Ciências da Informação e da Gestão da Informação, com destaque para a Curadoria da Informação". À vista disso, cabe esclarecer as principais áreas que fundamentam a GCI.

A definição de ciência da informação, segundo Bawden e Robinson (2012), não é facilmente estabelecida devido à sua multidisciplinaridade. Ela pode estar voltada aos estudos da computação e tecnologia da informação, ou estar relacionado com a teoria da informação, ou ainda, estar voltada à documentação e aos registos informacionais. Contudo, para este estudo, assim como Bawden e Robinson (2012), o foco está na terceira descrição, fundamentada por Saracevic (2010, p. 2570) ao descrever a ciência da informação como "the science and practice dealing with the effective collection, storage,

retrieval, and use of information"[2], além de interessar-se pelas tecnologias que facilitam o seu uso e gestão.

Pode ainda ser definida, segundo a *International Encyclopedia of Information and Library Science* como citado por Bottle (2003, p. 295)

> "A discipline that investigates the characteristics of information and the nature of the information transfer process, whilst not losing sight of the practical aspects of collecting, collating and evaluating information and organizing its dissemination through appropriate intellectual apparatus and technology."[3]

Resumindo, a ciência da informação apresenta meios para lidar com a informação de forma eficiente, sem esquecer o seu suporte e recursos necessários para tal. Ela utiliza-se das ferramentas provenientes da tecnologia da informação de maneira a melhorar a gestão e utilização da informação, adequando-a às necessidades dos utilizadores.

A GI possui diversas definições devido às diversas áreas que a estudam (Maceviciute & Wilson, 2002). Maceviciute e Wilson (2002) fizeram um estudo cronológico das principais definições e características da GI desde 1989 a 2000 e enfatizam a definição proposta por Wilson na *International Encyclopedia of Information and Library Science* em 1997 e atualizada em 2003, para:

> "The application of management principles to the acquisition, organization, control, dissemination and use of information relevant to the effective operation of organizations of all kinds. 'Information' here refers to all types of information of value, whether having their origin inside or outside the organization, including: data resources, such as production data; records and files related, for example, to the personnel function; market research data; and competitive intelligence from a wide range of sources. Information management deals with the value, quality, ownership, use and security of information in the context of organizational performance."[4] (Wilson, 2003, p. 263)

Complementando a descrição supra, Detlor (2010) caracteriza a GI como uma maneira de manter as pessoas e as organizações mais informadas para que realizem seus objetivos através do acesso e uso da informação de maneira eficiente e eficaz. Assim, por

[2] "a ciência e prática de lidar com coleções, armazenamento, recuperação e uso da informação de forma efetiva" (Saracevic, 2010, p. 2570 tradução nossa).
[3] "disciplina que investiga as características da informação e a natureza do processo de transferência da informação, sem perder de vista os aspetos práticos da recolha, classificação e avaliação da informação e organizar sua disseminação através de dispositivos intelectuais e tecnológicos apropriados" (Bottle, 2003, p. 295 tradução nossa).
[4] "A aplicação de princípios de gestão à aquisição, organização, controlo, disseminação e uso de informações relevantes para o funcionamento eficaz de organizações de todos os tipos. "Informações" aqui refere-se a todos os tipos de informações de valor, tenham sua origem dentro ou fora da organização, incluindo: recursos de dados, como dados de produção; registros e arquivos relacionados, por exemplo, à função de pessoal; dados de pesquisa de mercado; e inteligência competitiva de uma ampla variedade de fontes. A gestão de informações lida com o valor, qualidade, propriedade, uso e segurança das informações no contexto do desempenho organizacional". (Wilson, 2003, p. 263 tradução nossa).

meio da gestão de "processes and systems that create, acquire, organize, store, distribute, and use information"[5] (*ibdem*, p. 103) as pessoas e organização conseguiriam ser mais competitivas e estratégicas.

A GI não faz parte apenas dos processos operacionais de uma organização, apesar destes serem claramente fundamentais, dado que podem comprometer as características fundamentais dos materiais – autenticidade, confiabilidade, integridade e usabilidade (ISO, 2016)[6]. Ela visa também questões estratégicas da empresa, como a análise e estruturação de informações que auxiliem a tomada de decisões, a gestão do negócio e aos processos legais.

Já a CI, vem sendo realizada à muito tempo, mesmo que em outros formatos, ou por outros profissionais, como enfatiza Kim et al. (2013)

> "curation, which involves various activities that can help facilitate discovery, access, dissemination and archiving of information, is what librarians or archivists have done for hundreds of years. This implies that the similar skill sets used in traditional library work may be beneficial to curation work involving digital data and information"[7]. (Kim et al., 2013, p. 68)

Hoje, a CI está voltada predominantemente para o ambiente digital (Abbott, 2008; Higgins, 2011; Kim et al., 2013; Poole, 2013), visto o fenómeno do *Big data*, implicando a necessidade de renovação de técnicas e conhecimentos adquiridos até o momento. Com isso, cabe expor que a curadoria digital visa a manutenção, preservação e agregação de valor aos dados em todo o ciclo de vida da informação (Digital Curation Centre, 2020). Ela garante que os dados digitais estejam preservados e mediante uma gestão constante dos recursos evita a obsolescência tecnológica, além de reduzir ameaças à perda de valor dos recursos a longo prazo (Abbott, 2008). Pennock (2007) aponta que a curadoria vem, não somente para manter o valor da informação que já existe, mas acrescentar valor a ela a cada passo do seu ciclo de vida, por meio da sua gestão e avaliação, ou seja, a CI atua em prol às necessidades dos atuais e futuros interessados.

---

[5] "processos e sistemas que criam, adquirem, organizem, armazenem, distribuam e utilizem a informação" (Detlor, 2010 tradução nossa)

[6] Cabe ressaltar que a ISO 15489:2016 que discorre sobre a gestão de documentos (records), compreende estas características vinculadas à gestão de documentos, contudo nesta pesquisa a definição de documentos está alinhada à definição de informação tangível (vide 2.1).

[7] "curadoria envolve várias atividades que ajudam a facilitar a descoberta, acesso, disseminação e arquivamento de informações, é o que bibliotecários ou arquivistas têm feito há centenas de anos. Isso implica que os conjuntos de habilidades semelhantes usados no trabalho tradicional da biblioteca podem ser benéficos para o trabalho de curadoria envolvendo dados e informações digitais". (Kim et al., 2013, p. 68 tradução nossa)

A CI, em resumo, assegura a sustentabilidade dos dados para o futuro, não deixando de conferir valor imediato a eles para os seus criadores e para os seus utilizadores. Os recursos estratégicos, metodológicos e tecnológicos envolvidos nas práticas da CI facilitam o acesso persistente a dados digitais confiáveis por meio da melhoria da qualidade desses dados, do seu contexto de pesquisa e do controlo da autenticidade (Sayão & Sales, 2012).

Concluindo, pode-se inferir que a GCI é a área que visa a sustentabilidade dos dados para uso dos interessados de acordo com as suas necessidades, além de agregar valor à informação por meio de sua seleção, tratamento e distribuição. E que, assim como enfatiza Higgins (2018), quanto à curadoria digital, conforme o amadurecimento da disciplina novos conceitos e processos vão surgir. Vale ainda ressaltar que, o Mestrado em GCI proporciona o desenvolvimento de competências e habilidades interdisciplinares que são necessárias para o novo cenário mundial.

3.1 Ciclo de vida da informação

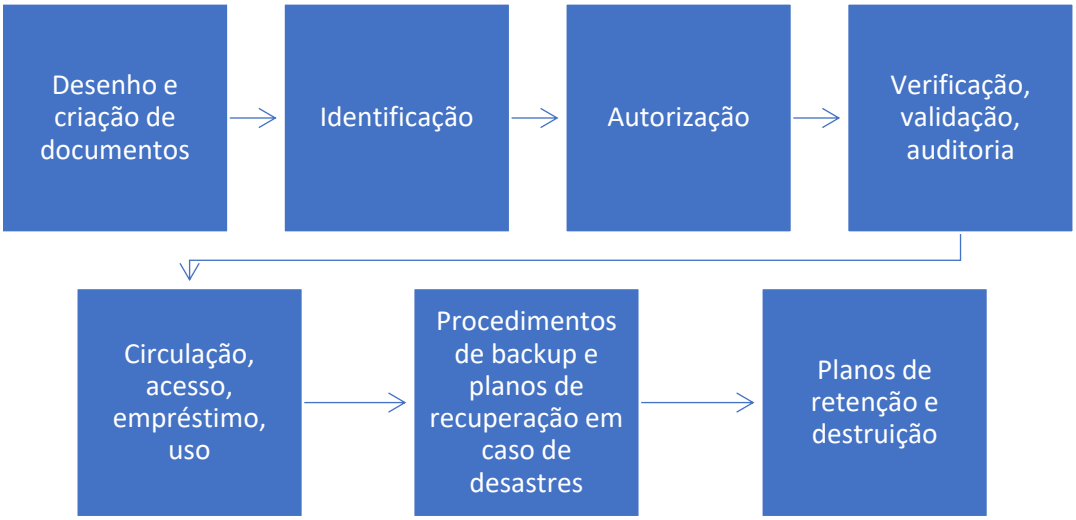
Uma das principais formas de gestão, além de ser uma das abordagens mais comuns na GCI é referente à identificação das etapas do ciclo de vida da informação. Essa abordagem permite a melhor visualização dos processos, atividades e relacionamentos da informação. Além de permitir uma melhor gestão a longo prazo (Higgins, 2007), ela também assegura a manutenção da autenticidade, confiabilidade, integridade e usabilidade de materiais digitais (Higgins, 2008). A importância dessa abordagem, segundo Pennock (2007, p. 2), está ligada, principalmente a três fatores:

1. A fragilidade dos materiais digitais e a obsolescência tecnológica;
2. Todas as ações realizadas nos estágios do ciclo de vida influem na gestão e preservação dos materiais; e
3. A autenticidade e integridade dos materiais deve ser mantida, por meio da curadoria, para a utilização e reutilização dos materiais.

O autor (*ibdem*) ainda aponta que essa abordagem facilita a continuidade de acesso aos materiais e valida a proveniência do material digital, independentemente das mudanças ocorridas no contexto ou organização de criação, mas que nem sempre é possível implementar todas as etapas do ciclo de vida.

Antes de apresentar alguns modelos do ciclo de vida da informação, cabe esclarecer que, compreender a informação e todo o caminho por ela percorrido é uma abordagem realizada em diversas áreas, como a biblioteconomia, museologia, arquivística, curadoria, entre outras. Na arquivística, por exemplo, Wilson (2003) cita o trabalho realizado por Goodman (1994), que apresenta as etapas para o ciclo de vida dos documentos de arquivos e como é fundamental para a gestão (figura 2).

Figura 2 - *Ciclo de vida dos documentos de arquivo.*

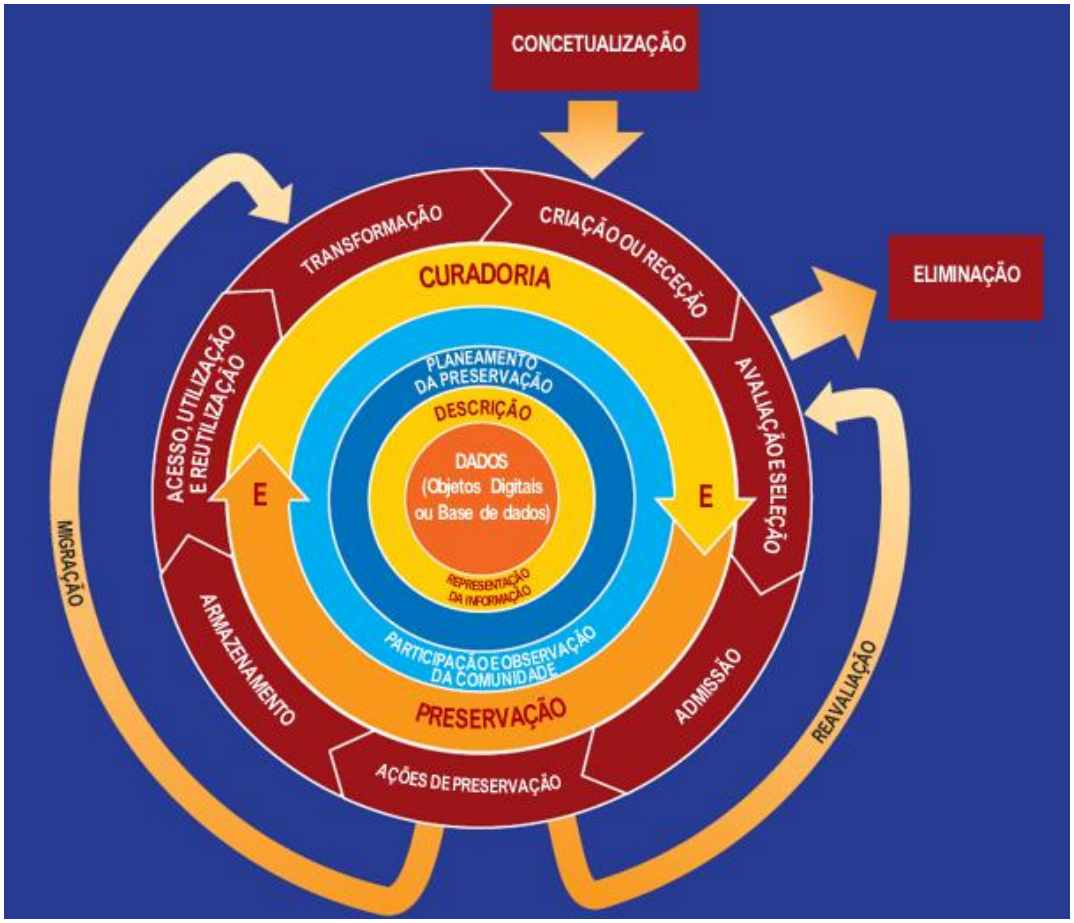


Fonte: Adaptado de Goodman (1994).

Em 2007, Sarah Higgins apresentou em seu artigo, *"Draft DCC Curation Lifecycle Model"* um esboço desenvolvido por ela e por outros estudiosos da área de curadoria digital, por meio do DCC (*Digital Curation Centre* - centro de pesquisa especializado em curadoria digital), de um modelo de curadoria do ciclo de vida da informação direcionado à curadoria digital. Segundo ela, esse modelo apresenta uma visão geral de todos os estágios necessários para curar e preservar de forma eficiente os materiais digitais desde a sua concetualização (Higgins, 2007). Ademais, por ser um modelo holístico, este apresenta a funcionalidade de visualização de todos os estágios sequencialmente, facilitando assim a definição de funções e responsabilidades, como também a criação de normas e tecnologias para o implementar e da documentalização dos processos.

Desde a sua concetualização, esse modelo tem sido adaptado e aprimorado e segundo Higgins (2008), por ser um modelo que apresenta uma visão geral, pode ser adaptado e alterado dependendo da necessidade da organização a utilizá-lo, assim como pode ser implementado em conjunto com outros modelos e normas, para maior granularidade das etapas. Atualmente, em 2020, o DCC apresenta o modelo a seguir (figura 3), que pode ser dividido em três partes: a primeira relativa às ações do ciclo de vida completo, a segunda referente às ações sequenciais e a terceira voltada às ações ocasionais.

Figura 3 - *Modelo de curadoria do ciclo de vida da informação DCC.*



Fonte: Traduzido de DCC Curation Lifecycle Model | Digital Curation Centre (2020).

Além do modelo, foi elaborada uma tabela detalhada, traduzida e adaptada do *DCC Curation Lifecycle Model | Digital Curation Centre* (2020), contendo as descrições das ações e suas definições (tabela 2).

Tabela 2 - *Ações do ciclo de vida completo.*

AÇÕES DO CICLO DE VIDA COMPLETO	
Ação	**Descrição**
Descrição e Representação da informação	Atribuir metadados administrativos, descritivos, técnicos, estruturais e de preservação, usando padrões adequados, para garantir uma descrição e controlo adequados a longo prazo. Recolher e atribuir a representação da informação necessárias para entender e apresentar o material digital e os metadados associados.
Planeamento da preservação	Planear a preservação durante todo o ciclo de vida da curadoria do material digital. Isso incluiria planos para a gestão e administração de todas as ações do ciclo de vida de curadoria.
Participação e observação da comunidade	Acompanhar as atividades apropriadas da comunidade e participar do desenvolvimento de padrões, ferramentas e *software* adequados.
Curadoria e preservação	Estar ciente e realizar ações administrativas e de gestão planeadas para promover a curadoria e preservação durante todo o ciclo de vida da curadoria.

Fonte: Traduzido de DCC Curation Lifecycle Model | Digital Curation Centre (2020)

As ações do ciclo de vida completo são as ações centrais apresentadas no modelo. Estão assim expostas porque são ações que devem ocorrer de maneira contínua durante todo o processo de curadoria. Elas também são consideradas as ações estratégicas do modelo. Em seguida, na tabela 3, serão apresentadas as ações sequenciais.

Tabela 3 - *Ações sequenciais*

AÇÕES SEQUENCIAIS	
Ação	**Descrição**
Concetualização	Conceber e planear a criação de dados, incluindo o método de captura e opções de armazenamento.
Criação ou receção	Criar dados, incluindo metadados administrativos, descritivos, estruturais e técnicos. Os metadados de preservação podem também ser adicionados no momento da criação. Receber dados, de acordo com as políticas de recolha documentadas, de criadores de dados, outros arquivos, repositórios ou centros de processamento de dados e, se necessário, atribuir metadados apropriados.
Avaliação e seleção	Avaliar e selecionar os dados para curadoria e preservação a longo prazo. Seguir as orientações, políticas ou requisitos legais documentados.
Admissão	Transferir dados para um arquivo, repositório, centro de processamento de dados ou para outro custodiante. Seguir as orientações, políticas ou requisitos legais documentados.
Ação de preservação	Realizar ações para garantir a preservação e retenção a longo prazo da natureza autorizada dos dados. As ações de preservação devem garantir que os dados permaneçam autênticos, confiáveis e utilizáveis, mantendo a sua integridade. As ações incluem a limpeza, a validação, a designação de metadados de preservação, a designação de informações de representação e a garantia de estruturas de dados ou formatos de arquivo aceitáveis.
Armazenamento	Armazenar os dados de forma segura, seguindo os padrões relevantes.
Acesso, utilização e reutilização	Garantir que os dados estejam acessíveis diariamente, tanto para utilizadores designados quanto para reutilizadores. Isto pode ser na forma de informações publicadas disponíveis de forma pública. Controlos de acesso e procedimentos de autenticação robustos podem ser aplicáveis.
Transformação	Criar novos dados a partir do original, por exemplo: • pela migração para um formato diferente; ou • criando um subconjunto, por seleção ou consulta, para criar novos resultados derivados, talvez para publicação.

Fonte: Traduzido de DCC Curation Lifecycle Model | Digital Curation Centre (2020)

As ações sequenciais são executadas repetidamente durante o processo de CI, garantindo a execução das estratégias centrais do modelo, ou seja, são as ações operacionais. Na tabela 4, serão apresentadas as ações ocasionais.

Tabela 4 - *Ações ocasionais.*

AÇÕES OCASIONAIS	
Ação	**Descrição**
Eliminação	Descartar os dados que não foram selecionados para curadoria e preservação a longo prazo, de acordo com políticas, orientações ou requisitos legais documentados. Normalmente, os dados podem ser transferidos para outro arquivo, repositório, centro de processamento de dados ou para outro custodiante. Em alguns casos, os dados são destruídos. A natureza dos dados pode, por razões legais, exigir destruição segura.
Reavaliação	Retornar dados que falhem nos procedimentos de validação para avaliação e re-seleção posterior.
Migração	Migrar dados para um formato diferente. Isso pode ser feito de acordo com o ambiente de armazenamento ou para garantir a imunidade dos dados à obsolescência de *hardware* ou *software*.

Fonte: Traduzido de DCC Curation Lifecycle Model | Digital Curation Centre (2020).

Ações ocasionais são as que serão realizadas dependendo da demanda. Elas são realizadas entre as ações sequenciais, reordenando-as conforme a necessidade da organização.

É importante frisar que outros modelos do ciclo de vida da informação foram desenvolvidos ao longo dos anos (Ball, 2012; Faundeen et al., 2014; Humphrey, 2006; Kowalczyk, 2017), muitas vezes também conhecido como ciclo de vida dos dados. Contudo, como apresenta Pouchard (2015) ao desenvolver um novo modelo, apesar da diferença nas descrições, uns por serem mais específicos ou abrangentes, outros por serem

mais flexíveis ou mais estáticos, todos os modelos visam a curadoria e preservação da informação a longo prazo.

A aplicabilidade de cada modelo depende de cada organização e das suas necessidades, ou seja, de certa forma, as necessidades dos interessados devem ser asseguradas desde o estudo e o planeamento de utilização do modelo. A utilização de abordagens de modelos do ciclo de vida da informação simplifica visualmente um complexo e dinâmico processo de gestão e curadoria das informações de uma organização.

3.2 Normas ISO referentes à Ciência da Informação

Associações como a *International Organization for Standardization* (ISO - Organização Internacional para Padronização) e a *International Electrotechnical Commission* (IEC - Comissão Eletrotécnica Internacional) desenvolvem por meio de um comité de especialistas, normas técnicas, classificações e normas de procedimentos, de forma a assegurar a sistematização de métodos e processos em diversas áreas.

Referente à área de ciência da informação, o que inclui temas como documentação, biblioteconomia e sistema de arquivos, a ISO possui a esta data 101 normas publicadas (ISO, 2020). Destas, vinte e cinco estão relacionadas à GI, apresentando a definição de conceitos, princípios, avaliações e processos de implementação, gestão e melhorias para diferentes tipos de arquivos, bibliotecas e centros de documentação. A seguir apresenta-se uma lista destas:

- **ISO 15489-1:2016 -** Information and documentation — Records management — Part 1: Concepts and principles;
- **ISO 16175-1:2020 -** Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records;
- **ISO 16175-2:2011 -** Information and documentation — Principles and functional requirements for records in electronic office environments — Part 2: Guidelines and functional requirements for digital records management systems;

- **ISO 18829:2017 -** Document management — Assessing ECM/EDRM implementations — Trustworthiness;
- **ISO/TR 19814:2017 -** Information and documentation — Collections management for archives and libraries;
- **ISO/TR 19815:2018 -** Information and documentation — Management of the environmental conditions for archive and library collections;
- **ISO/TR 21946:2018 -** Information and documentation — Appraisal for managing records;
- **ISO/TR 21965:2019 -** Information and documentation — Records management in enterprise architecture;
- **ISO 22310:2006 -** Information and documentation — Guidelines for standards drafters for stating records management requirements in standards;
- **ISO/TR 22428-1 -** Information and documentation — Records management in the cloud — Part 1: Issues and concerns;
- **ISO 23081-1:2017 -** Information and documentation — Records management processes — Metadata for records — Part 1: Principles;
- **ISO 23081-2:2009 -** Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues;
- **ISO/TR 23081-3:2011 -** Information and documentation — Managing metadata for records — Part 3: Self-assessment method;
- **ISO 24610-1:2006 -** Language resource management — Feature structures — Part 1: Feature structure representation;
- **ISO 24610-2:2011 -** Language resource management — Feature structures — Part 2: Feature system declaration;
- **ISO 24619:2011 -** Language resource management — Persistent identification and sustainable access (PISA);
- **ISO/TS 24620-1:2015 -** Language resource management — Controlled natural language (CNL) — Part 1: Basic concepts and principles;
- **ISO/DIS 24620-3 -** Language resource management — Controlled human communication (CHC) — Part 3: Basic principles and methodology for controlled oral communication (COralCom);
- **ISO 24622-1:2015 -** Language resource management — Component Metadata Infrastructure (CMDI) — Part 1: The Component Metadata Model;

- **ISO 24622-2:2019 -** Language resource management — Component metadata infrasctructure (CMDI) — Part 2: Component metadata specification language;
- **ISO/TR 26122:2008 -** Information and documentation — Work process analysis for records;
- **ISO/TR 26122:2008/COR 1:2009 -** Information and documentation — Work process analysis for records — Technical Corrigendum 1;
- **ISO 30300:2020 -** Information and documentation — Records management — Core concepts and vocabulary;
- **ISO 30301:2019 -** Information and documentation — Management systems for records — Requirements;
- **ISO 30302:2015 -** Information and documentation — Management systems for records — Guidelines for implementation.

Como apontado, estas normas voltadas à GI abordam diversas características deste processo, mas no que concerne à gestão de documentos, a norma ISO 15489-1:2016 é uma das mais conhecidas e aplicadas. Isto deve- se ao facto dela apresentar os conceitos e princípios da gestão de documentos, como os sistemas de arquivos, as políticas, as responsabilidades, a avaliação, os controlos e os processos para a criação, a captação e a gestão dos documentos (ISO, 2016). Inicialmente esta norma foi publicada em 2001 e em 2016 foi revista e novamente publicada. Segundo Indolfo (2007, p. 42), esta norma está voltada aos "processos que garantem um sistemático controlo da produção, uso, manutenção e eliminação de documentos. Ela é aplicável a todo documento de arquivo, independentemente do suporte material e da entidade produtora".

Também sobre processo de trabalho, a norma ISO/TR 26122:2008 fornece orientação sobre a análise do processo de trabalho quanto à perspetiva da criação, da captura e do controlo de registros (ISO, 2008). Contudo, esta apresenta orientações sobre uma pequena parte do processo de gestão.

Relativo à implementação de sistemas de gestão de documentos de arquivo (SGDA), as normas ISO 30300:2020, ISO 30301:2019 e ISO 30302:2015 fornecem orientações sobre os conceitos, os requisitos e as diretrizes para a sua implementação. Sobre os sistemas de gestão, Ruesta (2012) define-os como "o conjunto de elementos

interrelacionados ou que interagem numa organização com o fim de estabelecer políticas e objetivos, bem como os processos para os alcançar". Desta forma, estas normas que incidem sobre os sistemas de gestão objetivam as boas práticas de negócio, além de fornecer a Alta Administração uma ferramenta verificável e controlável por meio de uma abordagem sistemática (ABNT, 2016).

3.3 Sistema de Gestão de Documentos de Arquivo

Não existe nenhum normativo para um sistema de GI genérico. No entanto existe um normativo de referência para a gestão de documento de arquivo, um aspeto particular da gestão de informação que na realidade acaba por ser suficiente em grande parte dos casos para representar as principais preocupações da GI.

Publicada pela primeira vez em 2011, a norma ISO 30301 foi revista e alterada em 2019. Esta norma apresenta os requisitos para o desenvolvimento e a implementação de um SGDA, além de fornecer informações quanto o monitoramento e mensuração de seu desempenho. Apresentada a seguir, a norma ISO 30301:2019 está dividida em 11 seções, sendo as seções 0 a 3 introdutórias e não obrigatórias na aplicação, além de possuir um anexo e bibliografia (ISO, 2019).

0. **Introdução:** Introduz a norma e explica a compatibilidade com as outras normas.
1. **Âmbito:** Explica a característica genérica da norma e a sua aplicabilidade com outras normas.
2. **Referências normativas:** Refere-se à norma ISO 30301:2019 e à definição de termos da norma.
3. **Termos e definições:** Refere-se à norma ISO 30301:2019 e à definição de terminologia.
4. **Contexto da organização:** Definição dos requisitos para o entendimento de assuntos externos e internos, partes interessadas, expectativa da organização e a definição do escopo do SGDA.
   - 4.1. **Entendendo a organização e o seu contexto:** Requisitos para o entendimento da organização no contexto interno e externo.

4.1.1. **Geral:** Apresenta informações gerais sobre os requisitos da organização e seu contexto.

4.1.2. **Requisitos dos documentos:** Determina os requisitos de análise dos documentos.

4.2. **Compreendendo as necessidades e expectativas das partes interessadas:** Determinação das partes interessadas e expectativas da organização.

4.3. **Determinando o âmbito do sistema de gestão de documentos de arquivo:** Determina a aplicação e limites do SGDA.

4.4. **Sistema de gestão de documentos de arquivo:** Etapas que devem ser seguidas e mantidas pela organização, ou seja, um processo contínuo.

5. **Liderança:** Determina o envolvimento e tarefas a serem desenvolvidas pelos líderes.

5.1. **Liderança e compromisso:** Envolvimento dos líderes e os seus papéis para o SGDA.

5.2. **Política:** Estabelecimento de uma política de documentos**.**

5.3. **Funções, responsabilidades e autoridades organizacionais:** Determinação das funções, responsabilidades e autoridades dentro do SGDA.

6. **Planeamento:** Planeamento das etapas relacionadas ao risco e aos objetivos do SGDA.

6.1. **Ações para lidar com riscos e oportunidades:** Determina ações a serem desenvolvidas em relação à avaliação de risco e oportunidades.

6.2. **Objetivos dos documentos e planeamento para alcançá-los:** Etapas a serem realizadas para a implementação dos objetivos dos documentos.

7. **Suporte:** Requisitos relativos aos suportes necessários na implementação do SGDA.

7.1. **Recursos:** Determinação dos recursos necessários.

7.2. **Competência:** Determinação das competências necessárias.

7.3. **Consciência:** Apresenta os documentos, procedimentos e outros itens que devem ser apresentados aos envolvidos no SGDA.

7.4. **Comunicação:** Determina o quê, quando, como e quem deve ser comunicado sobre os processos do SGDA.

7.5. **Informação documentada:** Determina formas de lidar com a informação documentada do SGDA, desde a criação, atualização, controlo, armazenamento, entre outros.

7.5.1. **Geral:** Determina aspetos gerais do SGDA.

7.5.2. **Criação e atualização:** Determina processos de criação e atualização da documentação.

7.5.3. **Controlo da documentação:** Determina procedimentos quanto ao controlo dos documentos.

8. **Operação:** Apresenta os procedimentos operacionais do SGDA.

8.1. **Planeamento e controlo operacional:** Requerimentos para o planeamento e implementação do controlo operacional.

8.2. **Determinando arquivos a serem criados:** Determina a criação da documentação de processos.

8.3. **Desenho e implementação de processos, controlos e sistemas de arquivos:** Desenvolvimento e implementação dos processos de documento.

9. **Avaliação de desempenho:** Avaliação e monitoramento dos processos do SGDA.

9.1. **Monitoramento, medição, análise e avaliação:** Determina o quê, quem, quando e como deve ser monitorado, medido, analisado e avaliado o desempenho do SGDA.

9.2. **Auditoria interna:** Apresenta os aspetos para a auditoria do SGDA.

9.3. **Revisão da administração:** Determinação de revisão do SGDA pelos gestores.

10. **Melhoria:** Apresenta ações de melhoria para os processos.

10.1. **Não conformidade e ação corretiva:** Determina ações quanto às atividades que apresentam não conformidade e ações corretivas.

10.2. **Melhoria contínua:** Determina a continuidade da melhoria dos processos impostos na norma.

Anexo A (normativo) Requerimentos operacionais para processos, controlos e sistemas de arquivos: Controlos que podem ser implementados mediante necessidade da organização.

Bibliografia: Referências bibliográficas utilizadas para desenvolvimento da norma.

Isto posto, cabe ressaltar que está descrito na própria norma ISO 30301:2019 que a sua estrutura é holística e desenvolvida de maneira a ser compatível com a utilização de outras normas (ISO, 2019). Ademais, a sua implementação deve ser realizada em conjunto com as normas da família ISO 30000 – a norma ISO 30300:2020 que define os principais conceitos, apresenta o vocabulário utilizado e a norma ISO 30302:2015 que apresenta diretrizes para a implementação do SGDA, oferecendo suporte de alto nível.

Desta forma, para uma organização a gestão de documentos voltada ao ciclo de vida dos documentos é primordial e, como explana Indolfo (2007), esta vem influenciar quanto a eficiência, a eficácia e a qualidade nos negócios. Ademais, a utilização das normas ISO em conjunto com os processos da CI constituem uma sólida estrutura para o desenvolvimento de negócios, auxílio à tomada de decisões e melhoria contínua de processos.

4. Segurança da Informação

A SI caracteriza-se, de acordo com a norma ISO/IEC 27000 (2018, p. 4), pela "preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved"[8]. Ela deve ser garantida para que se minimize os riscos envolvidos nos processos de negócios (Dantas, 2011). A SI deve ser aplicada através de políticas, educação, consciencialização, treinamento e tecnologia, seja no armazenamento, processamento, transmissão ou uso da informação (Whitman & Mattord, 2016). Entende-se a SI como um processo extenso e de contínua avaliação e aperfeiçoamento. Whitman e Mattord (2016, p. 23) complementam que:

> "Even with the best planning and implementation, it is impossible to obtain perfect information security. […] Information security cannot be absolute: it is a process, not a goal. You can make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information. On the other hand, a completely secure information system would not allow anyone access"[9].

Em outras palavras, a SI é um processo contínuo, que possui diversas etapas. Ela deve ser desenvolvida observando as necessidades da organização e seu contexto, de maneira a melhor salvaguardar os seus recursos. A seguir serão apresentados os principais conceitos da SI, os fatores que compõem um sistema de gestão de segurança da informação (ISMS) e o processo da SI.

4.1 Conceitos da Segurança da Informação

Existem três características fundamentais na SI: a confidencialidade (*confidentiality)*, integridade (*integrity)* e disponibilidade (*availability*). A garantia do triângulo C.I.A - (*confidentiality*, *integrity and availability*) (Whitman & Mattord, 2016), como também é conhecido o conjunto dessas três características-, por medidas de SI

[8] "garantia da confidencialidade, integridade e disponibilidade da informação. Somado a estas, outras propriedades como a autenticidade, responsabilidade, não repúdio e confiabilidade podem também estar envolvidas". (ISO/IEC, 2018, p. 4 tradução nossa)

[9] "Mesmo com o melhor planeamento e implementação, é impossível obter uma segurança da informação perfeita. […] A segurança da informação não pode ser absoluta: é um processo, não uma meta. Você pode disponibilizar um sistema para qualquer pessoa, em qualquer lugar, a qualquer hora e por qualquer meio. No entanto, esse acesso irrestrito representa um perigo para a segurança da informação. Por outro lado, um sistema de informação completamente seguro não permitiria que ninguém o acedesse."(Whitman & Mattord, 2016, p. 26 tradução nossa)

valorizam a organização, pois lhe dão mais credibilidade, mitigando os riscos de perdas de informações essenciais e o comprometimento de recursos.

A confidencialidade da informação pode ser caracterizada por ser a garantia de que a informação não será disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados (ISO/IEC, 2018, p. 2). Ela garante que a informação mantém o seu valor (Dantas, 2011). Um exemplo de incidente relacionado com a quebra da confidencialidade da informação, aconteceu no ataque de um hacker à empresa Capital One de cartões de crédito, que o fez ter acesso a mais de 100 milhões de contas e aplicações (McLean, 2019).

Já a integridade é a garantia de que a informação está completa, inteira, sem alterações, consistente e não esteja corrompida de nenhuma maneira (Campos, 2014; Dantas, 2011; ISO/IEC, 2018; Whitman & Mattord, 2016). É exemplo de ataque à integridade da informação, o ato que ocorreu em 2019 em Nassau, nas Bahamas, quando o Ministério do Turismo sofreu de um ataque de vírus que acabou corrompendo diversos dos seus arquivos (Moxey, 2019).

A disponibilidade, entretanto, garante que a informação esteja disponível e possa ser acedida a qualquer momento, sem interferências ou interrupções, pelo indivíduo ou entidade que esteja autorizado (ISO/IEC, 2018; Whitman & Mattord, 2016). A disponibilidade é assegurada ao garantir "o êxito da leitura, do trânsito e do armazenamento da informação" (Dantas, 2011, p. 13). Ataques de *ransomware* (*softwares* maliciosos que restringem o acesso ao sistema que foi infetado, solicitando pagamento para sua liberação («Ransomware», 2020)) são os ataques mais comuns que afetam a disponibilidade da informação. Um exemplo foi o ataque ao Weather Channel nos Estados Unidos em 2019, que acabou alterando a programação do canal (Mathews, 2019).

Contudo, com as mudanças no cenário da tecnologia, outras características deveriam, segundo Whitman e Mattord (2016), entrar na lista de características a serem protegidas, como a exatidão, a autenticidade, a utilidade e a propriedade (von Solms & van Niekerk, 2013). Whitman e Mattord (2016) definem estes termos da seguinte forma:

- Exatidão (*accuracy*): é o atributo que garante que a informação está livre de erros e possui o valor que o utilizador espera;
- Autenticidade (*authenticity*): é a garantia que a informação é original e não produto de reproduções;

- Utilidade (*utility*): o atributo que garante que a informação tem o valor ou utilidade para a qual foi criada; e
- Propriedade (*possession*): garante que a posse ou controlo da informação foi autorizado ou é legítimo.

Os procedimentos de SI devem ser aplicados em todos os processos de um sistema de informação de uma organização. Esse sistema é composto pelas seguintes partes (Whitman & Mattord, 2016):

- *Software*: como aplicações e sistemas operacionais;
- *Hardware*: ativos físicos da organização que armazenam *software*s e dados;
- *Dados*: todos os dados e informações da organização, estando na forma física ou digital;
- *Pessoas*: pessoas ligadas à organização que devem ser educadas e treinadas de maneira a evitar que elas danifiquem ou percam informações;
- *Procedimentos*: todas instruções desenvolvidas pela organização para o desenvolvimento de tarefas, como manuais, normas e até mesmo procedimentos não verbais; e
- *Redes*: conjunto de sistemas de informações conectados entre si.

Com o desenvolvimento de técnicas de proteção dos atributos da informação e considerando as vulnerabilidades existentes do ativo informacional é possível minimizar a ocorrência de incidentes de SI.

Segundo a norma ISO/IEC 27000 (2018), os incidentes de SI podem ser definidos como um evento, ou uma série de eventos indesejados ou inesperados que de alguma forma venham a aumentar significativamente a probabilidade de comprometer as operações de negócios e ameaçar a SI. As ameaças, o risco, a probabilidade, o impacto que aquele incidente pode causar e qual controlo pode ser realizado devem ser ponderados e previstos pela organização. Desta forma, expõe-se adiante o que caracteriza estes cinco fatores.

A norma ISO/IEC 27000 (2018, p. 10) define ameaça como "potential cause of an unwanted incident, which can result in harm to a system or organization"[10]. A

[10] "causa potencial de um incidente indesejado, que pode resultar em danos a um sistema ou organização" (ISO/IEC, 2018, p. 10 tradução nossa)

categorização dessas ameaças advém de sua natureza, podendo ser classificada de diversas maneiras. Whitman e Mattord (2016) desenvolveram 12 categorias que representam perigo ao sistema de informação de uma organização, apresentados na tabela 5 a seguir:

Tabela 5 - *Ameaças ao sistema de informação.*

Categoria da ameaça	**Exemplos de ataque**
Comprometimento da propriedade intelectual	Pirataria, violação de direitos autorais
Divergência na qualidade de serviço	Problemas de funcionamento do provedor de serviços de Internet (ISP), energia ou WAN
Espionagem ou invasão	Acesso não autorizado e/ou recolha de dados
Forças da natureza	Incêndios, inundações, terremotos, raios
Erro humano ou falha	Acidentes, erros dos funcionários
Extorsão de informações	Chantagem, divulgação de informações
Sabotagem ou vandalismo	Destruição de sistemas ou informações
Ataques de *software*	Vírus, *worms*, macros, negação de serviço
Falhas ou erros técnicos de *hardware*	Falha no equipamento
Falhas ou erros técnicos de *software*	Erros, problemas de código, brechas desconhecidas
Obsolescência tecnológica	Tecnologias antiquadas ou desatualizadas
Roubo	Confisco ilegal de equipamentos ou informações

Fonte: Traduzido de Whitman e Mattord (2016, p. 52).

Cabe evidenciar que dependendo da estrutura, característica e estratégia organizacional de cada organização, essas ameaças devem ser consideradas de maior ou menor probabilidade de ocorrer. Esse tipo de análise faz parte da análise do risco que a instituição deve realizar.

A análise do risco, juntamente com a identificação do risco e seu controlo, fazem parte da gestão do risco, como apontam Whitman e Mattord (2016).

> "Initially, the organization must identify and understand the risk it faces, especially the risk to information assets. Once identified, risk must be assessed, measured, and evaluated. The key determination is whether the risk an organization faces exceeds its comfort level. If not, the organization is satisfied with the risk management process. Otherwise, the organization needs to do something to reduce risk to an acceptable level."[11] (Whitman & Mattord, 2016, p. 231)

Os autores também apresentam as etapas que compõe a gestão do risco:

- **Identificação do risco**:
  - Identificar, inventariar e categorizar os ativos;
  - Classificar, avaliar o valor e priorizar os ativos;
  - Identificar e priorizar as ameaças;
  - Especificar as vulnerabilidades dos ativos.
- **Análise do risco**:
  - Determinar a frequência de perda;
  - Avaliar a magnitude da perda;
  - Calcular o risco;
  - Avaliar a aceitabilidade do risco.
- **Controlo do risco**:
  - Selecionar estratégias de controlo;
  - Justificar os controlos;
  - Implementar, monitorar e avaliar os controlos.

Dessa forma, é possível perceber que a gestão do risco é um processo complexo e que por si só, demanda muita atenção dos gestores da organização, mas é um dos processos mais importantes da SI. Campos (2014) enfatiza a importância na escolha dos colaboradores que farão parte da análise de risco da organização. Dado que essa equipa irá estudar os pontos fortes e fracos da organização, deve ser composta, preferencialmente, por pessoas de setores distintos e de total confiança, já que trabalharão

[11] "Inicialmente, a organização deve identificar e entender o risco que enfrenta, especialmente o risco para os ativos de informação. Uma vez identificado, o risco deve ser aferido, medido e avaliado. A principal determinação é se o risco que uma organização enfrenta excede seu nível de conforto. Se não, a organização está satisfeita com o processo de gerenciamento de riscos. Caso contrário, a organização precisa fazer algo para reduzir o risco a um nível aceitável." (Whitman & Mattord, 2016, p. 231 tradução nossa)

com informações sensíveis. O autor ainda ressalta a importância da aplicação de termos de sigilo e confidencialidade para estes colaboradores, devido a relevância desse trabalho.

Em relação à probabilidade da concretização de um incidente de SI, Campos (2014) aponta que há uma relação entre o grau da vulnerabilidade do ativo de informação com as ameaças. Diversos autores apresentam fórmulas matemáticas variadas para a definição da probabilidade, contudo, todos concordam que é muito difícil determinar o valor exato da probabilidade do incidente de SI, dado que os fatores que compõem essa equação são subjetivos. Para exemplificar esse tópico, Campos (2014) apresenta a seguinte situação:

> "[…] se considerarmos a queda de um meteoro nas proximidades de determinada organização uma ameaça, concordaremos que a probabilidade de isto acontecer é algo próximo a zero. No entanto, seria um erro afirmar que neste caso a probabilidade é zero. […] Existem ameaças consideradas de alto grau, como os vírus de computador, e as ameaças de baixo grau, como os meteoros que podem cair na superfície da terra. Existem também as vulnerabilidades de alto grau, como uma rede local de computadores ligadas à internet, e as vulnerabilidades de baixo grau, como um armário sem tranca para guardar o *backup* na sala dos computadores servidores (*datacenter).* Mas esses graus são sempre relativos, ou seja, mesmo as mais baixas vulnerabilidades poderão representar probabilidades consideráveis se o grau de ameaça for muito grande". (Campos, 2014, p. 27)

Para a definição da probabilidade, deve-se então fazer uma análise primária das vulnerabilidades e ameaças e então analisar a ocorrência dos incidentes. Contudo, para esse cálculo, deve-se considerar também o impacto que um incidente pode causar na organização.

O impacto é relativo aos prejuízos causados à organização. Esses prejuízos podem ser financeiros, perda ou insatisfação de colaboradores e clientes, risco à imagem da organização, entre outros. Ou seja, qualquer impacto que desvalorize a organização ou a prejudique de alguma forma.

Isto posto, cabe ainda realizar o controlo de forma que se minimize o impacto às organizações. Segundo Campos (2014, p. 28), o controlo é "um mecanismo utilizado para diminuir a fraqueza ou vulnerabilidade de um ativo". Alguns exemplos de controlo que podem ser realizados são senhas de acesso, políticas de SI, utilização de antivírus, criptografia, entre outros.

Como apresentado, a SI é um processo composto por diversas etapas e procedimentos variáveis, pois dependem das necessidades das organizações e como estas se estabelecem.

4.2 Sistema de Gestão de Segurança da Informação

Após a realização dos processos de análise da SI, a organização deve definir um plano de SI. Esse plano definirá todos os elementos que compõe e implementam a SI, como políticas, treinamento, controlos, entre outros. Geralmente, esses planos são baseados em modelos e normas que ajudam a definir os principais procedimentos, podendo ser adaptáveis dependendo da necessidade da organização.

Apesar de existirem outras normas relativas à tecnologia da informação, as normas "da família" ISO/IEC 27000 servem, especificamente, de diretrizes visando desde a definição de termos técnicos da área até à elaboração e gestão de projetos de sistemas de SI. Em outras palavras, estas normas definem um Sistema de Gestão de Segurança da Informação (ISMS – *Information security management systems*), que segundo a norma ISO/IEC 27000 (ISO/IEC, 2018), consiste em

> "An ISMS consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's information security to achieve business objectives. It is based on a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks. Analysing requirements for the protection of information assets and applying appropriate controls to ensure the protection of these information assets, as required, contributes to the successful implementation of an ISMS."[12] (ISO/IEC, 2018, pp. 11–12)

A seguir, apresenta-se uma lista das principais normas da família 27000 e suas designações nas áreas da Tecnologia da informação — Técnicas de segurança (*About the ISO27k standards*, 2020; ISO/IEC, 2018):

Normas gerais e vocabulário

- ISO/IEC 27000 - Information technology — Security techniques — Information security management systems — Overview and vocabulary.

[12] "Um ISMS consiste nas políticas, procedimentos, diretrizes e recursos e atividades associados, gerenciados coletivamente por uma organização, na busca de proteger seus ativos de informação. Um ISMS é uma abordagem sistemática para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança das informações de uma organização para atingir os objetivos de negócios. Baseia-se em uma avaliação de risco e nos níveis de aceitação de risco da organização projetados para tratar e gerenciar efetivamente os riscos. A análise de requisitos para a proteção de ativos de informação e a aplicação de controlos apropriados para garantir a proteção desses ativos de informação, conforme necessário, contribuem para a implementação bem-sucedida de um ISMS". (ISO/IEC, 2018, pp. 11–12)

Normas que especificam requisitos

- ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements;
- ISO/IEC 27006 - Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems;
- ISO/IEC 27009 - Information technology — Security techniques — Sector-specific application of ISO/IEC 27001 — Requirements;
- ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.

Normas que descrevem diretrizes gerais

- ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls;
- ISO/IEC 27003 - Information technology — Security techniques — Information security management —Guidance;
- ISO/IEC 27004 - Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation;
- ISO/IEC 27005 - Information technology — Security techniques — Information security risk management;
- ISO/IEC 27007 - Information technology — Security techniques — Guidelines for information security management systems auditing;
- ISO/IEC TR 27008 - Information technology — Security techniques — Guidelines for auditors on information security controls;
- ISO/IEC 27013 - Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1;
- ISO/IEC 27014 - Information technology — Security techniques — Governance of information security;
- ISO/IEC TR 27016 - Information technology — Security techniques — Information security management — Organizational economics;
- ISO/IEC 27021 - Information technology — Security techniques — Information security management — Competence requirements for information security management systems professionals.

Normas que descrevem diretrizes específicas do setor

- ISO/IEC 27010 - Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications;
- ISO/IEC 27011 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations;

- ISO/IEC 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- ISO/IEC 27018 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;
- ISO/IEC 27019 - Information technology — Security techniques — Information security controls for the energy utility industry;
- ISO 27799 - Health informatics — Information security management in health using ISO/IEC 27002.

Como exposto, existem diversas normas que são modelos para a implementação de um ISMS. Elas abrangem diversos aspetos da implementação e boas práticas a serem seguidas e podem ser adaptadas de acordo com a necessidade da organização em sua implementação. É importante destacar que, por enquanto, somente a norma ISO/IEC 27001 pode ser certificada pela ISO. Esta certificação é uma forma de assegurar aos clientes e consumidores que as melhores práticas foram adotadas e de que os processos de SI estão sendo seguidos.

4.3 O processo da segurança da informação

As organizações realizam diversas atividades no seu quotidiano. Essas atividades precisam ser identificadas e geridas para que obtenham resultados mais eficazes e eficientes. O conjunto de atividades interrelacionadas, que podem ser mensuradas de maneira a obter resultados consistentes e previsíveis, pode ser denominada processo. De acordo com a ISO, a definição de processo é:

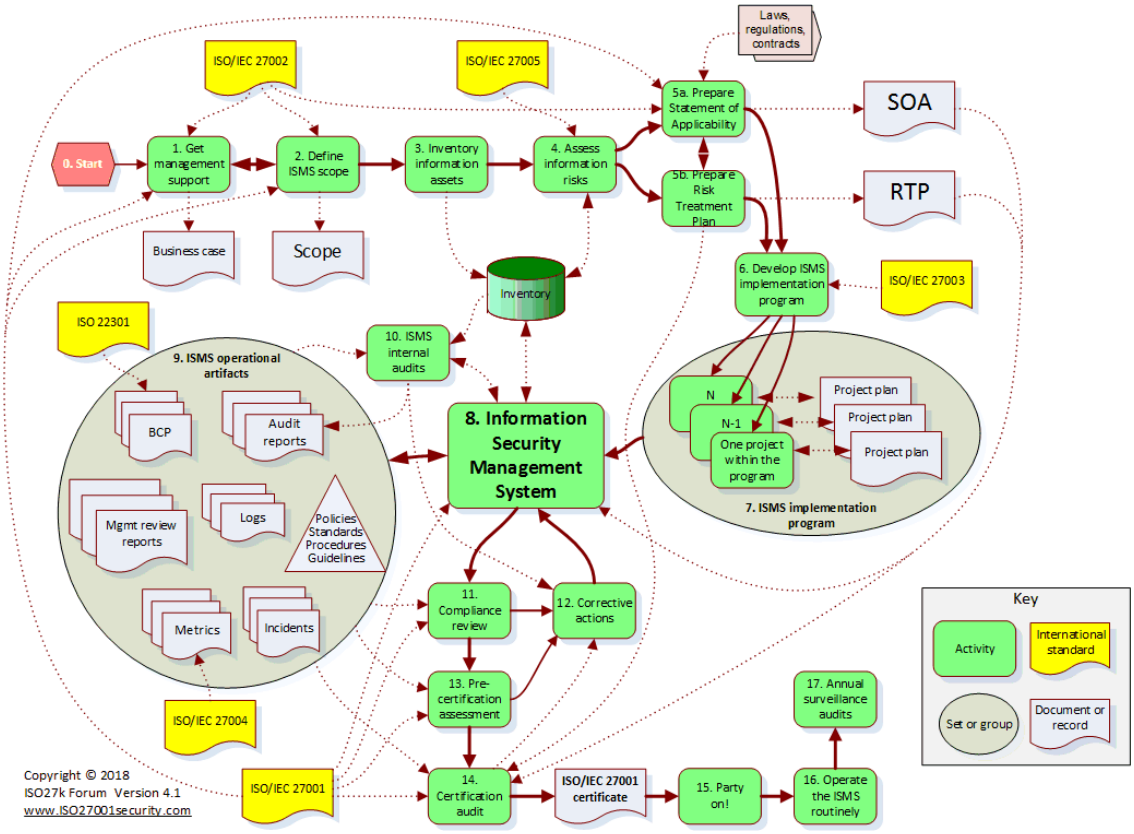
> Any activity using resources needs to be managed to enable the transformation of inputs into outputs using a set of interrelated or interacting activities; […]. The output from one process can directly form the input to another process and generally this transformation is carried out under planned and controlled conditions. The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach"[13]. (ISO/IEC, 2018, p. 13)

[13] "Qualquer atividade que utilize recursos precisa ser gerenciada para permitir a transformação de entradas em saídas usando um conjunto de atividades inter-relacionadas ou em interação; […]. A saída de um processo pode formar diretamente a entrada para outro processo e, geralmente, essa transformação é realizada sob condições planeadas e controladas. A aplicação de um sistema de processos dentro de uma organização, juntamente com a identificação e interações desses processos e seu gerenciamento, pode ser referida como uma "abordagem de processo""(ISO/IEC, 2018, p. 13 tradução nossa).

Estes processos podem ser encontrados nas organizações em diversas áreas. Em relação à SI, essa abordagem pode ser identificada em âmbito coletivo e individual. Âmbito coletivo refere-se à aplicação de processos em conjunto, um exemplo pode ser encontrado na figura 4 [retirada de Free ISO27k Toolkit (iso27001security, 2020)] , que apresenta a implementação e certificação de um ISMS, ao utilizar diversas normas da família ISO 27000.

Nesta abordagem é possível identificar as diversas atividades que o compõem e como as normas as influenciam. É importante destacar que cada norma *per se* possui outro conjunto de processos a serem aplicados, de maneira que este ciclo é integrado e contínuo.

Figura 4 - *Fluxograma de implementação e certificação de um ISMS utilizando as normas da família ISO27k.*



Fonte: Free ISO27k Toolkit (iso27001security, 2020).

Todavia, quando a abordagem de processos é aplicada em âmbito individual, significa que este processo pode ser analisado separadamente, como por exemplo, ao identificar as etapas do processo de implementação singular da norma ISO/ IEC 27001.

Esta é a norma mais conhecida e que apresenta os requisitos para o estabelecimento, implementação, manutenção e melhoramento de um ISMS.

Lançada em 2005 e baseada na Norma Britânica BS 7799-2, esta norma foi revista em 2013 e 2019, contudo a versão de 2013 ainda se mantém atual. Esta norma está dividida em 11 seções, sendo as seções 0 a 3 introdutórias e não obrigatórias na aplicação, além de possuir um anexo e bibliografia. Apresenta-se a seguir a estrutura da norma, as suas seções e definições (ISO/IEC, 2019).

0. **Introdução:** Introduz a norma e explica a compatibilidade com as outras normas.
1. **Âmbito:** Explica a característica genérica da norma e a sua aplicabilidade com outras normas.
2. **Referências normativas:** Refere-se à norma ISO 27000 e à definição de termos da norma.
3. **Termos e definições:** Refere-se à norma ISO 27000 e à definição de terminologia.
4. **Contexto da organização:** Definição dos requisitos para o entendimento de assuntos externos e internos, partes interessadas, expectativa da organização e a definição do escopo do ISMS.
    - 4.1. **Entendendo a organização e o seu contexto:** Requisitos para o entendimento da organização no contexto interno e externo.
    - 4.2. **Compreendendo as necessidades e expectativas das partes interessadas:** Determinação das partes interessadas e expectativas da organização.
    - 4.3. **Determinando o âmbito do sistema de gestão de segurança da informação:** Determina a aplicação e limites do ISMS.
    - 4.4. **Sistema de gestão de segurança da informação:** Etapas que devem ser seguidas e mantidas pela organização, ou seja, um processo contínuo.
5. **Liderança:** Determina o envolvimento e tarefas a serem desenvolvidas pelos líderes.
    - 5.1. **Liderança e compromisso:** Envolvimento dos líderes e os seus papéis para o ISMS.
    - 5.2. **Política:** Estabelecimento de uma política de segurança de informação**.**

5.3. **Funções, responsabilidades e autoridades organizacionais:** Determinação das funções, responsabilidades e autoridades dentro do ISMS.

6. **Planeamento:** Planeamento das etapas relacionadas ao risco e aos objetivos da segurança da informação.
   - 6.1. **Ações para lidar com riscos e oportunidades:** Determina ações a serem desenvolvidas em relação à avaliação e tratamento do risco.
   - 6.2. **Objetivos de segurança da informação e planeamento para alcançá-los:** Etapas a serem realizadas para a implementação dos objetivos da segurança da informação.
7. **Suporte:** Requisitos relativos aos suportes necessários na implementação do ISMS.
   - 7.1. **Recursos:** Determinação dos recursos necessários.
   - 7.2. **Competência:** Determinação das competências necessárias.
   - 7.3. **Consciência:** Apresenta os documentos, procedimentos e outros itens que devem ser apresentados aos envolvidos no ISMS.
   - 7.4. **Comunicação:** Determina o quê, quando, como e quem deve ser comunicado sobre os processos do ISMS.
   - 7.5. **Informação documentada:** Determina formas de lidar com a informação documentada, desde a criação, atualização, controlo, armazenamento, entre outros.
8. **Operação:** Apresenta os procedimentos operacionais para atingir a segurança da informação.
   - 8.1. **Planeamento e controlo operacional:** Requerimentos para o planeamento e implementação do controlo operacional.
   - 8.2. **Avaliação de risco à segurança da informação:** Determina a execução da avaliação de risco.
   - 8.3. **Tratamento de riscos à segurança da informação:** Implementação do plano de tratamento de risco à segurança da informação.
9. **Avaliação de desempenho:** Avaliação e monitoramento dos processos de segurança da informação.
   - 9.1. **Monitoramento, medição, análise e avaliação:** Determina o quê, quem, quando e como deve ser monitorado, medido, analisado e avaliado o desempenho da segurança da informação.

9.2. Auditoria interna: Apresenta os aspetos para a auditoria da segurança da informação.

9.3. Revisão da administração: Determinação de revisão do ISMS pelos gestores.

10. Melhoria: Apresenta ações de melhoria para os processos.

10.1. Não conformidade e ação corretiva: Determina ações quanto às atividades que apresentam não conformidade e ações corretivas.

10.2. Melhoria contínua: Determina a continuidade da melhoria dos processos impostos na norma.

Anexo A (normativo) Objetivos e controlos de controlo de referência: Controlos que podem ser implementados mediante necessidade da organização. Apresentados também na norma ISO/IEC 27002.

Bibliografia: Referências bibliográficas utilizadas para desenvolvimento da norma.

Em suma, a ISO/IEC 27001, dividida em diversas seções, apresenta um plano de implementação de um ISMS. Com isso, ela garante que os ativos informacionais se mantenham seguros, além de garantir os princípios da SI: confidencialidade, integridade e disponibilidade. Os processo da SI podem ser aplicados em âmbito coletivo ou singular. Contudo, mesmo que aplicado singularmente, não significa que sua complexidade é melhor, dado que um processo é composto por diversas atividades que podem ser de maior ou menor complexidade.

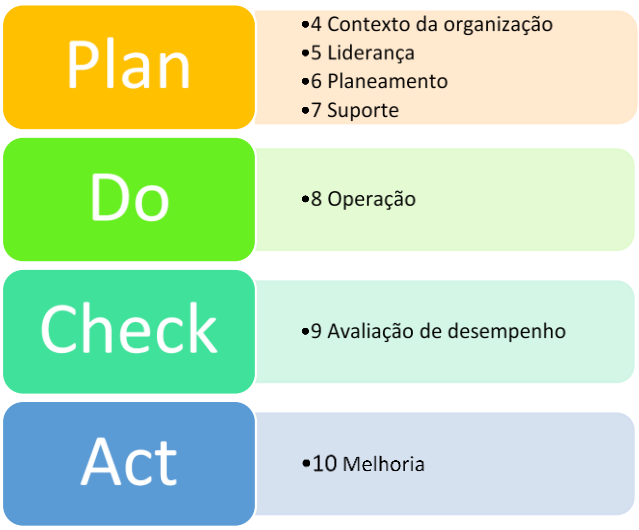
5. Modelo concetual

Como apresentado na introdução, esta pesquisa possui como objetivo desenvolver um alinhamento entre os processos da SI com os da GCI. Para atender aos objetivos propostos e responder à questão de investigação foram formuladas três hipóteses que alavancaram o desenvolvimento dessa pesquisa.

Assim como mencionado, os objetivos da SI são: proteger os ativos informacionais, por meio da utilização de processos, arquivamento, manutenção e uso dos ativos informacionais para que a organização possa alcançar os seus objetivos (ISO/IEC 27000, 2018). Os objetivos da GI podem ser resumidos em: prover acesso à informação às pessoas e organizações de maneira a mantê-las mais informadas e para que possam atingir os seus objetivos (Detlor, 2010). E os objetivos da CI atuam em prol dos interessados através da: manutenção, preservação e agregação de valor aos dados em todo o seu ciclo de vida por meio da gestão de recursos (Digital Curation Centre, 2020).

Ambas as áreas de SI e GI propõem sistemas de gestão, considerando as etapas do ciclo PDCA (Plan - Do - Check - Act) (ver figura 5).

Figura 5 – *Etapas do PDCA e as normas ISO/IEC 27001 e ISO 30301.*



Fonte: Elaboração própria

O ciclo PDCA criado por William Edwards Deming na década de 1950, é uma ferramenta de gestão com desenvolvimento contínuo que visa alinhar os processos de

atividade dentro de uma cadeia de valor. Segundo Velasco et al (2018), o PDCA garante a confidencialidade, integridade e disponibilidade das informações. Este método baseia-se em quatro passos, a saber (Johnson, 2016; Moen & Norman, 2006; Sokovic et al., 2010):

1) **Plan –** Planear uma mudança que vise uma melhoria;
2) **Do –** Fazer a mudança (preferencialmente em pequena escala);
3) **Check –** Conferir os resultados e verificar pontos positivos e negativos;
4) **Act –** Adotar ou abandonar a mudança, dependendo dos resultados, e voltar a realizar o ciclo.

Mediante aos argumentos expostos, é possível inferir que, por possuírem objetivos, objeto de foco e pontos de interesse em comum, possuem certos processos que se podem alinhar. Isto posto, levantou-se a **hipótese 1:**

- *A GI e a SI possuem processos que se podem alinhar.*

Devido à GCI ser uma área muito nova e em desenvolvimento e não possui métodos e processos próprios, ela apropria-se dos processos dos campos de estudo dos quais deriva: a GI e a CI. Ainda no que concerne à GI e a CI, sabe-se que ambas possuem processos estabelecidos e, se considerado a gestão de documentos como sinónimo da GI, baseando-se na definição de informação tangível apresentada no capítulo 2, acrescenta-se esta ao leque de normas que dão suporte à área. Essas normas, desenvolvidas por um conjunto de especialistas, têm como objetivo assegurar a padronização dos processos.

Outra área a se destacar em relação ao desenvolvimento e aplicação de normas é a SI, que por ser uma área já estabelecida, possui diversas normas desenvolvidas pela ISO (como abordado no capítulo 4) e que estão em constante atualização de modo a contemplar as mudanças que ocorrem na sociedade, como por exemplo, a norma ISO/IEC 27701 (ISO/IEC, 2019) uma extensão da norma ISO/IEC 27001 (ISO/IEC, 2013a) e que visa a gestão da informação privada em conformidade com os novos tópicos discutidos na atualidade como o Regulamento Geral sobre a Proteção de Dados (RGPD, 2016).

É diante desse contexto que se destaca que dado a GCI ser fundamentada em áreas bem estruturadas, e utilizando-se também do modelo da SI, por possuírem certos objetivos semelhantes, o desenvolvimento de normas da GCI que garantissem a

padronização da aplicação dos processos, melhoraria a sua aplicabilidade. Assim, levanta-se a **hipótese 2:**

- *O estabelecimento de normas da GCI podem melhorar a sua aplicabilidade.*

Segundo o Dicionário Priberam da Língua Portuguesa (Priberam, 2008a), eficácia é o efeito de produzir algo, de tornar real, enquanto a eficiência (Priberam, 2008b) é a capacidade de produzir um efeito, de produzir com o mínimo de erros ou de meios, é também sinónimo de competência. Assim, na realização de tarefas é possível ser eficaz e não eficiente e vice-versa. A realização de uma tarefa é o sinónimo de eficácia, contudo as organizações buscam além. Requerem que as ações sejam eficientes de maneira a poupar recursos e, consequentemente, aumentar o ROI (retorno de investimento) das empresas. Devido à congruência de objetivos das duas áreas em estudo, deduz-se que o alinhamento de seus processos e práticas melhoraria a eficácia e a eficiência. Um exemplo pode ser observado ao analisar o ciclo de vida da informação proposto pelo DCC (Digital Curation Centre, 2020) na figura 1 e o processo de classificação de informação.

Ao realizar a comparação das etapas do ciclo de vida da informação com o processo de classificação de informação descrito por Gouveia (2016), no qual deve-se identificar o ativo informacional, classificá-lo, rotulá-lo e tomar precauções quanto ao manuseio da informação, nota-se que certas etapas se assemelham:

Tabela 6 - *Comparação por amostragem.*

Ciclo de vida da informação	**Processo de classificação da informação**
Criar ou receber	-
Avaliar e selecionar	Identificação
	Classificação
Admissão	Rotulação
Ação de preservação	Manipulação e manuseio da informação
Armazenar	

Aceder, usar e reutilizar	[Desde a descrição sobre processos de segurança quanto ao armazenamento, transmissão, novas formas de classificação (caso necessário) e descarte das informações]
Transformar	-

Fonte: Elaboração própria

Como verificado, etapas descritas como Avaliação e seleção possuem parte dos processos como Identificação e Classificação descritos por Gouveia (2016). E outras etapas não descritas no processo de classificação da informação, mas descritos no ciclo de vida da informação como o Transformar, poderiam ser utilizados em conjunto, o que aumentaria a eficácia e eficiência da aplicação dos processos em organizações.

Isto posto, utilizando este processo como amostra, deduz-se que em maior escala, ou seja, numa análise da norma ISO/IEC 27001 que apresenta os requisitos para a implementação de um ISMS, com a norma ISO 30301 e com o modelo desenvolvido pelo DCC, é possível fazer um alinhamento entre eles de maneira a melhorar a eficácia e eficiência na sua aplicação conjunta. Dessa forma, levantou-se a **hipótese 3:**

- *Há uma relação positiva em termos de melhoria na eficácia e eficiência quando a GCI e a SI são aplicadas em conjunto.*

Assim, com o levantamento destas três hipóteses e utilizando-se da metodologia abaixo descrita, foi possível alavancar esta pesquisa.

6. Metodologia

Assim que a sociedade avança e novas descobertas são feitas, é necessário a realização de pesquisas científicas de modo a cobrir áreas de interesse e preocupação social (Bryman, 2012). Utilizando técnicas de pesquisas sociais, este estudo pretende preencher uma lacuna na literatura científica em âmbitos sociais e tecnológicos.

Uma abordagem epistemológica interpretativa foi escolhida para conduzir esta pesquisa. Segundo Bryman (2012) uma abordagem epistemológica é aquela que reflete sobre o que é, ou deveria ser, considerado para estudo numa disciplina. O autor aponta duas doutrinas a serem consideradas quanto à epistemologia da pesquisa: o positivismo e o interpretativo. O positivismo afirma que métodos aplicados às ciências naturais devem ser utilizados para estudar as ciências sociais e afins, em outras palavras, fatores como o estudo de fenómenos e conhecimentos confirmados, formulação de hipóteses testáveis, entre outros. Já o interpretativo, segundo o autor, apoia-se no facto de as ciências naturais serem diferentes das sociais, requerendo-se assim, procedimentos específicos e diferentes dos aplicáveis às ciências naturais. Resumidamente, o positivismo tenta explicar o comportamento humano, enquanto o interpretativo tenta entendê-lo (Bryman, 2012). Isto posto, é importante apontar que esta pesquisa se desenvolve sob a posição ontológica construtivista. Dado que o construtivismo visa o entendimento, a construção social e a geração de teorias sobre o estudo que está sendo realizado (Creswell, 2014).

Por não existirem estudos específicos que analisem os temas desta pesquisa em conjunto, decidiu-se, portanto, proceder com uma pesquisa de cunho exploratório. Esse tipo de pesquisa, segundo Marconi e Lakatos (2003) e Santos e Candeloro (2006), intendem identificar padrões e objetiva a formulação de um problema de pesquisa, a fim de aumentar a familiaridade do tema/ objeto de análise de pesquisa com o pesquisador e proporcionar-lhe uma ampla visão sobre o assunto, para a clarificação de conceitos e para o desenvolvimento de pesquisas futuras.

Quanto à abordagem da pesquisa, foi escolhido o método qualitativo, dado que este visa o entendimento e exploração de temas de cunho social (Creswell, 2014). O método qualitativo pode possuir diversos designs como estudo de caso, abordagem fenomenológica, narrativa, entrevistas, método comparativo, etc. (Creswell, 2014; Marconi & Lakatos, 2003). O método comparativo, que visa a análise das semelhanças e diferenças de grupos e assuntos estudados (Marconi & Lakatos, 2003) foi o escolhido como design da pesquisa.

Utilizou-se a técnica de pesquisa documental, cuja a principal fonte de recursos são documentos, escritos ou não (como áudios, vídeos e outros tipos de medias), como expõe Marconi e Lakatos (2003). Dessa forma, para o levantamento bibliográfico principal foram utilizados repositórios académicos e científicos como:

- B-on (https://www.b-on.pt/);
- Google Scholar (https://scholar.google.com/);
- Social Sciences Open Access Repository (https://www.gesis.org/en/ssoar/home/);
- Wiley Online Library (https://onlinelibrary.wiley.com/);
- Nova Discovery (https://www.fcsh.unl.pt/faculdade/bibliotecas/);
- RUN – Repositório da NOVA (https://run.unl.pt/);
- RCAAP – Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/); etc.

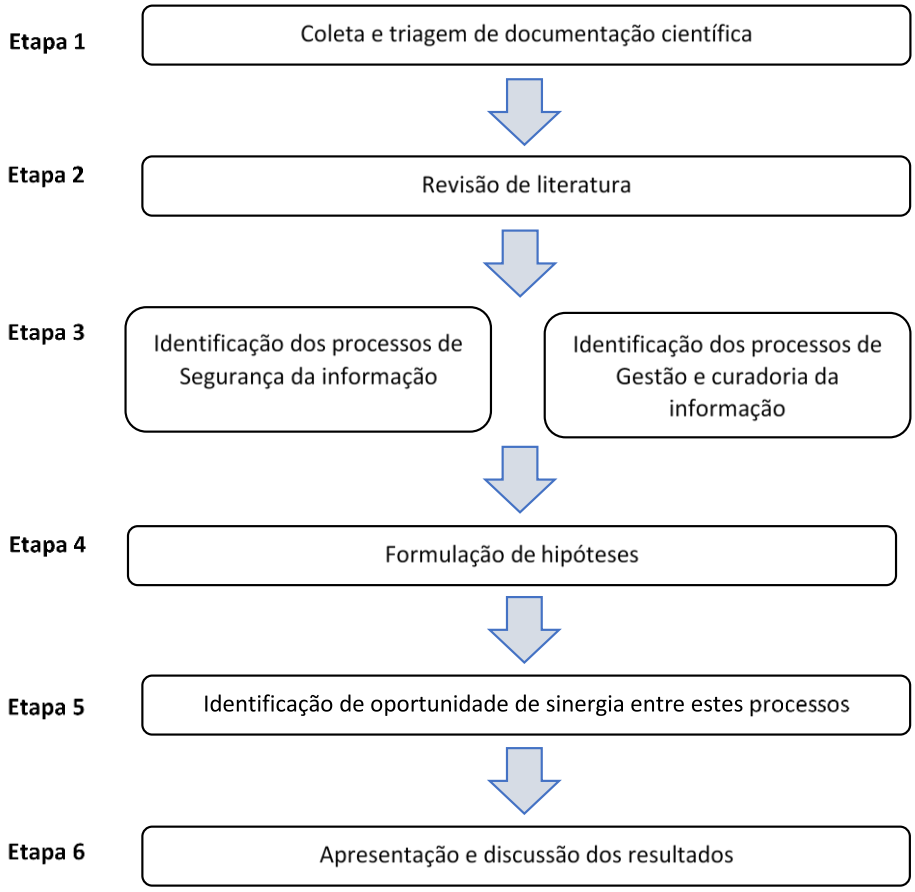
Além de pesquisas realizadas em jornais, revistas científicas e publicações específicas das áreas, em especial:

- Elsevier;
- International Organization for Standardization (ISO);
- Digital Curation Center (DCC); e
- Journal of Management Information Systems;

Para a realização da pesquisa nos motores de busca, foram utilizados termos correspondentes às áreas como “segurança da informação” e “gestão e curadoria da informação”. Devido às especificidades das buscas, outros termos relacionados, como “gestão da informação”, “curadoria da informação”, “gestão do conhecimento”, “segurança da informação em organizações”, entre outros foram utilizados, para ampliar a gama de resultados e proporcionar uma captação de literatura mais abrangente. É importante destacar que a pesquisa foi realizada nos idiomas português e inglês, isto porque a grande maioria das publicações encontram-se em inglês, mas também para verificar o que já havia sido publicado no idioma de partida do texto deste estudo e em publicações internacionais.

A figura 6 a seguir expõe as etapas do desenvolvimento desta pesquisa de forma a clarificar o atual processo de trabalho:

Figura 6 - *Etapas do desenvolvimento da pesquisa.*



Fonte: Adaptado de Centobelli et al. (2018).

- **Etapa 1:** Após a recolha primária de publicações, foi realizada uma análise dos resumos dos artigos e procedeu-se à classificação dos artigos por áreas de estudo, além da eliminação de materiais que não englobavam a delimitação dos temas ou conceitos explorados nesta pesquisa;
- **Etapa 2:** Revisão de literatura para a definição de conceitos pertinentes de maneira a esclarecer e delimitar a pesquisa;
- **Etapa 3:** Identificação dos processos de segurança da informação e GCI;
- **Etapa 4:** Formulação de hipóteses baseadas em insights retirados das etapas prévias;
- **Etapa 5:** Identificação de fatores que proporcionem o alinhamento dos processos previamente identificados; e
- **Etapa 6:** Apresentação e discussão dos resultados obtidos.

7. Análise comparativa dos processos

A fim de propor um alinhamento entre os processos de GCI (que se apropria dos processos da GI e CI) e os da SI, primeiramente foi necessário realizar a comparação destes, de modo a entender as suas semelhanças e diferenças. Devido aos diversos processos que existem nestas áreas de pesquisa, foi necessário, primeiramente, destacar um processo de cada área para poder iniciar as análises.

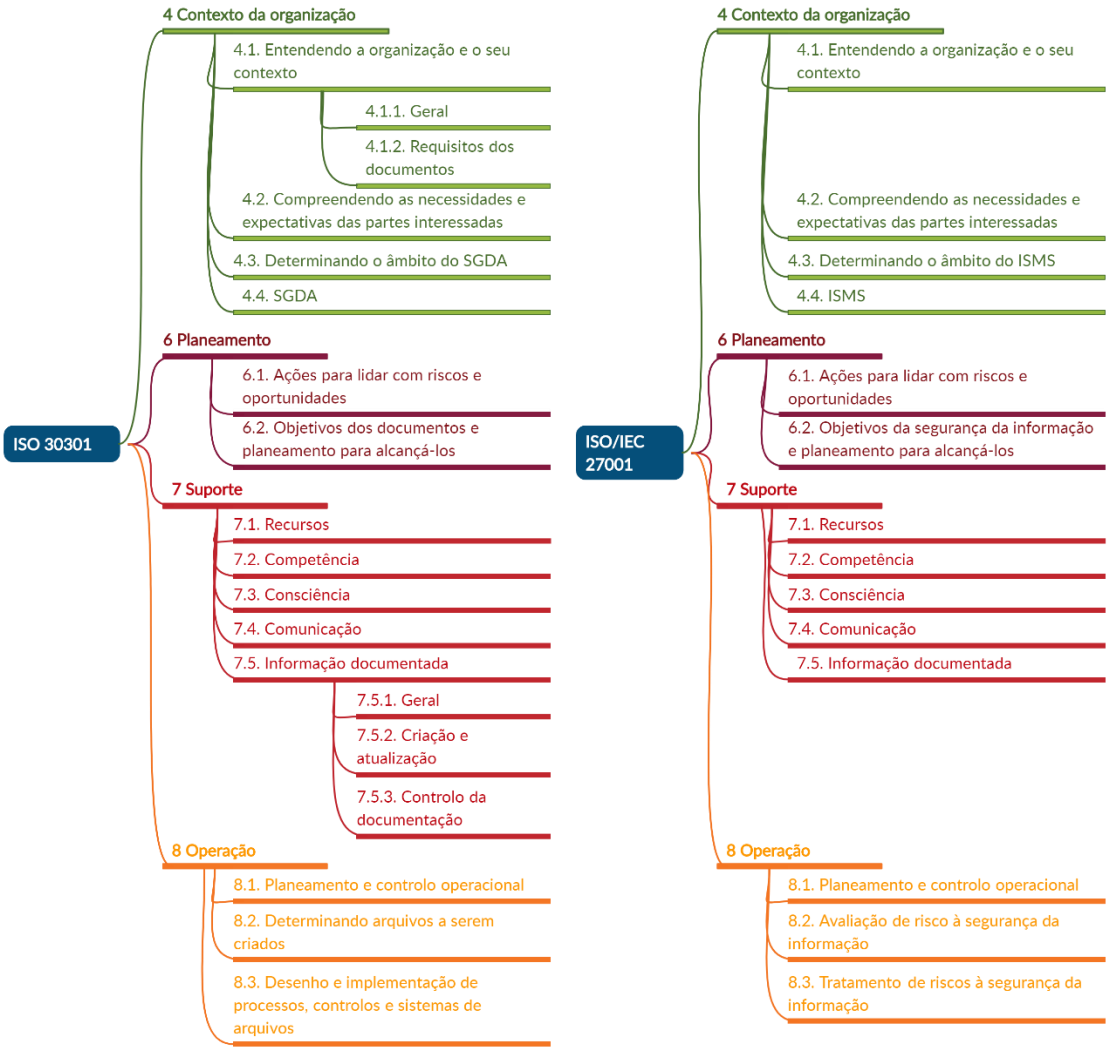
Desta forma, esta análise pretende ao comparar os processos descritos nos seguintes subcapítulos: o 3.1, o modelo do ciclo de vida da informação; o 3.3, requerimentos para a implementação de um SGDA descritos na norma ISO 30301; e o 4.3, o processo de aplicação de um ISMS descrito na norma ISO/IEC 27001. Para melhor visualização foi desenvolvida a figura 7 abaixo, exemplificando-os:

Figura 7 - *Processos de CI, GI e SI.*

Fonte: Elaboração própria

Pela figura 7 nota-se que a ISO 30301 possui uma estrutura igual à da ISO/IEC 27001. Indubitavelmente, que devido ao âmbito de aplicação de cada uma das normas as suas especificações irão diferenciar-se, contudo pouco se altera em sua estrutura geral. Este facto pode ser averiguado na figura 8, que apresenta as diferenças entre as normas. Ao considerar os referidos aspetos é importante ressaltar que a maior alteração entre ambas as normas é o acréscimo dos sub-subcapítulos (4.1.1, 4.1.2, 7.5.1, 7.5.2 e 7.5.3). Todas as outras mudanças são maioritariamente devido ao âmbito de aplicação, como previamente referido: ou por mudança de terminologia (como os itens 4.3 ou a seção 6, por exemplo) ou por processos específicos (como a seção 8)

Figura 8 – *Diferenças entre a ISO 30301 e a ISO/IEC 27001.*



Fonte: Elaboração própria

Devido ao paralelismo entre a estrutura das normas ISO 30301 e a ISO/IEC 27001, para evitar redundâncias de explicação na continuação da análise comparativa, decidiu-se por realizar uma análise aprofundada da ISO/IEC 27001 em detrimento da ISO 30301. Para a realização desta análise comparativa entre os processos, definiu-se alguns elementos de alto nível que nortearam a comparação. Estes foram escolhidos com base nos principais aspetos das áreas:

- Estrutura dos documentos;
- Linguagem e Expressividade;
- Completude;
- Flexibilidade;
- Envolvimento da alta administração; e
- Continuidade do processo e melhoria.

A seguir será detalhado cada um dos elementos mencionados, assim como serão realizados os comentários pertinentes à análise comparativa.

7.1 Estrutura dos documentos

A análise sobre a estrutura dos documentos visa avaliar a clareza na exposição dos temas e a forma que estão organizados.

Em relação à norma ISO/IEC 27001, ela é dividida em seções por área de aplicação. As quatro primeiras seções (da 0 à 3) são introdutórias. Explicam o âmbito, referências normativas e a terminologia utilizada na norma, o que facilita a compreensão e elucida dúvidas de aplicação. As outras seções são de aplicação da norma, propriamente dito, ou seja, apresentam os requisitos de implementação do ISMS por áreas de uma organização, como o contexto da organização, liderança, planeamento, suporte, operação, avaliação de *performance* e melhoria. Estas seções determinam ações a serem implementadas mediante cada um dos requisitos, além de exemplificar controlos nas próprias seções e no Anexo A. Um exemplo, é o abordado na seção 6.1.3 sobre tratamentos de risco da SI, que apresentam seis controlos, além de orientar a consulta do Anexo A, de maneira que nenhum dos controlos sejam negligenciados. É necessário enfatizar que apesar do Anexo A ser uma listagem à parte, é essencial na aplicação da norma, dado que muitos passos descritos no Anexo A não estão descritos em nenhum outro lugar da norma e são essenciais ao processo. Vale ainda ressaltar que quanto à

clareza na exposição das seções, a norma ISO/IEC 27001 está muito bem dividida. Dado este ser um documento de referência, estar claramente estruturada e de forma lógica facilita a consulta para a aplicação. Assim como a ISO/IEC 27001, a ISO 30301, possui a mesma estrutura, e dessa forma, a análise é equivalente.

O modelo do DCC, por outro lado, possui uma estruturação diferente, em relação à divisão de áreas de aplicação. Apesar do modelo apresentar suas atividades em forma circular, depreende-se que a sua leitura seja do interior para o exterior (ver figura 3). Contudo, a etapa concetualização encontra-se fora do círculo e aparenta ser a primeira etapa a ser realizada. Dessa forma, não fica claro no modelo que as ações centrais são estratégicas e devem ser realizadas antes da etapa concetualização, ou seja, este modelo cria uma ambivalência de aplicação, que pode ser confuso ao utilizar na organização.

Resumidamente, ambas as normas são mais completas e mais sequenciais, as suas atividades são subdivididas e apresentadas de maneira clara, já o modelo do DCC carece de uma subdivisão de tarefas, de forma que muitos pontos foram perdidos (ver o tópico 7.3) e a sua sequência de atividades não foi estruturada de maneira clara.

7.2 Linguagem e Expressividade

O aspeto Linguagem e Expressividade visa avaliar a capacidade de representação dos processos. Está voltado à clareza na exposição dos temas e às terminologias aplicadas, isto é, se as notações representam completamente as atividades sugeridas no processo.

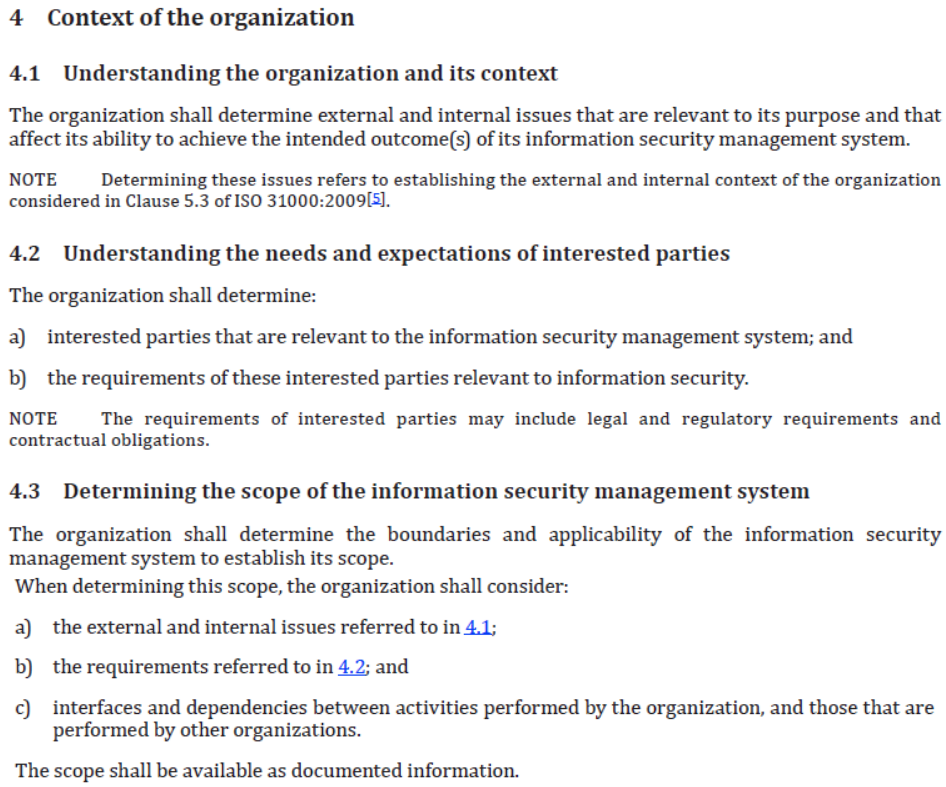
Apesar da norma ISO/IEC 27001 apresentar uma seção de termos e definições, não há nenhum termo definido nesta, pois leva à consulta de outra norma (ISO/IEC 27000). A norma ISO/IEC 27001 por si só não descreve a terminologia utilizada, o que pode dificultar no entendimento da aplicação para uma pessoa não qualificada. A ISO 30301, por outro lado, apresenta alguns termos na própria norma e enfatiza, contudo, a necessidade da utilização de outra norma de sua família: a norma ISO 30300.

À exceção deste ponto, a norma ISO/IEC 27001 mantém-se clara na abordagem de exposição das atividades, como por exemplo as descritas na seção 4 Contexto da organização (figura 9). Nesta seção (figura 9) é possível observar alguns aspetos como a subdivisão da seção, que clarifica as atividades que devem ser realizadas dentro deste componente. Ademais a descrição destas atividades faz-se de maneira clara e objetiva,

tornando-se, desta forma, menos ambígua. Em relação à sintaxe é possível identificar a utilização de três formas predominantes no inglês:

1. Forma contínua do verbo (*continuous*): para títulos, em geral, utiliza-se verbos finalizados em *-ing*, mostrando uma ação contínua;
2. Descritivo: procura descrever ações a serem realizadas ao longo do processo; e
3. Imperativo: as orações são construídas na forma imperativa pela utilização do verbo modal *shall*, que na terceira pessoa do singular expressa uma ordem ou sugestão.

Figura 9 - *Seção 4 da norma ISO/IEC 27001.*



4 Context of the organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in Clause 5.3 of ISO 31000:2009[5].

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system; and

b) the requirements of these interested parties relevant to information security.

NOTE The requirements of interested parties may include legal and regulatory requirements and contractual obligations.

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope.

When determining this scope, the organization shall consider:

a) the external and internal issues referred to in 4.1;

b) the requirements referred to in 4.2; and

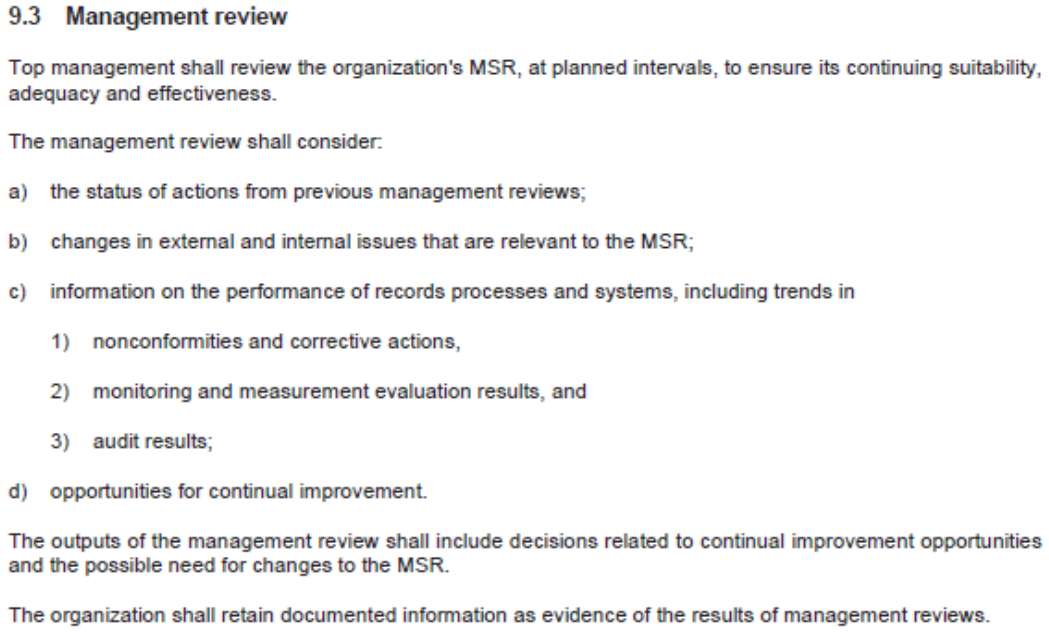
c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

The scope shall be available as documented information.

Fonte: ISO/IEC 27001 (ISO/IEC, 2013a, pp. 1–2).

Em relação à estrutura sintática e semântica, a norma ISO 30301 segue exatamente a mesma estrutura da norma ISO/IEC 27001, como apresentado na figura 10.

Figura 10 - *Seção 9.3 da norma ISO 30301.*



9.3 Management review

Top management shall review the organization's MSR, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

The management review shall consider:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the MSR;

c) information on the performance of records processes and systems, including trends in

1) nonconformities and corrective actions,

2) monitoring and measurement evaluation results, and

3) audit results;

d) opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and the possible need for changes to the MSR.

The organization shall retain documented information as evidence of the results of management reviews.

Fonte: ISO 30301 (ISO, 2019, p. 11).

As tabelas do modelo do DCC, da mesma forma, descrevem as atividades de forma clara e numa linguagem concisa (ver tabelas 2, 3 e 4). Esclarecem a terminologia utilizada, apontando as ações relativas a cada termo, utilizando-se de exemplos para eliminar ambivalências e duplicidade de termos. Muitos termos são cunhados na área da CI, descritos principalmente nos trabalhos de Chen et al. (2003), Dukes (2006), Pennock (2007), entre outros, como cita Higgins (2007, 2008). Em relação à sintaxe, pode-se observar o seguinte (tabela 7):

1. Forma padrão do verbo: para títulos, em geral, utiliza-se os verbos em sua forma padrão, ou seja, sem a utilização da partícula “to”;
2. Descritivo: procura descrever ações a serem realizadas ao longo do processo; e
3. Imperativo: as orações são construídas na forma imperativa pela utilização do verbo na forma padrão dele e sem a utilização do sujeito.

Tabela 7 - *Ações ocasionais em inglês.*

Occasional Actions	
Dispose	Dispose of data, which has not been selected for long-term curation and preservation in accordance with documented policies, guidance or legal requirements. Typically data may be transferred to another archive, repository, data centre or other custodian. In some instances data are destroyed. The data's nature may, for legal reasons, necessitate secure destruction.
Reappraise	Return data which fails validation procedures for further appraisal and reselection.
Migrate	Migrate data to a different format. This may be done to accord with the storage environment or to ensure the data's immunity from hardware or software obsolescence.

Fonte: Higgins (2008).

Em suma, os três documentos possuem uma linguagem não ambivalente, o que evita dúvidas de aplicação. A sua sintaxe é bem estruturada, utilizando-se da linguagem imperativa afirmativa e sempre seguindo a mesma estrutura. No geral, os documentos possuem linguagem clara e a notação dos termos é expressa de forma explícita.

7.3 Completude

Este aspeto pretende discorrer sobre a completude dos documentos, ou seja, se esta aborda elementos estratégicos, gerenciais e operacionais. Esta análise foi baseada nos trabalhos de Anthony (1965) e Gorry e Morton (1989), que visam a divisão de categorias que ajudam no planeamento e controlo pela gerência.

- Planeamento estratégico: "Strategic planning is the process of deciding on objectives of the organization, on changes in these objectives, and on the policies that are to govern the acquisition, use and disposition of these resources"[14] (1965 apud; Gorry & Morton, 1989).
- Controlo gerencial: "The processes by which managers assure that resources are obtained and used effectively and efficiently in the

[14] "O planeamento estratégico é o processo de decisão sobre os objetivos da organização, as mudanças nesses objetivos e as políticas que devem governar a aquisição, o uso e a disposição desses recursos". (1965 apud; Gorry & Morton, 1989 tradução nossa)

accomplishment of the organization's objective"[15] (1965 apud; Gorry & Morton, 1989).

- Controlo operacional: "The process of assuring that specific tasks are carried out effectively and efficiently"[16] (1965 apud; Gorry & Morton, 1989).

Dessa forma, categorizou-se as atividades descritas nas normas ISO/IEC 27001, ISO 30301 e no modelo do DCC da seguinte forma:

Tabela 8 - *Comparação sobre completude entre os documentos.*

	Normas ISO/IEC 27001 e ISO 30301	**Modelo do DCC**
Estratégico	○ 4 Contexto da organização ○ 5 Liderança ○ 6 Planeamento ○ 7 Suporte	○ Descrição e Representação da informação ○ Planeamento da preservação ○ Participação e observação da comunidade ○ Curadoria e preservação ○ Concetualização
Gerencial	○ 9 Avaliação de desempenho ○ 10 Melhoria	○ Eliminação ○ Reavaliação ○ Migração
Operacional	○ 8 Operação	○ Criação ou receção ○ Avaliação e seleção ○ Admissão ○ Ação de preservação ○ Armazenamento ○ Acesso, utilização e reutilização ○ Transformação

Fonte: Elaboração própria

[15] "O processo pelo qual os gestores asseguram que os recursos são obtidos e usados eficaz e eficientemente para alcançar os objetivos da organização". (1965 apud; Gorry & Morton, 1989 tradução nossa)
[16] "O processo de garantir que tarefas específicas sejam realizadas de maneira eficaz e eficiente".(1965 apud; Gorry & Morton, 1989 tradução nossa)

Nestes documentos, é possível categorizar as atividades segundo a proposta de Anthony (1965). Nota-se que, de maneira geral, os processos administrativos e gerenciais possuem a mesma quantidade de tópicos abordados, enquanto a categoria operacional é mais granulada no modelo do DCC. Contudo, apesar desta divisão, o modelo do DCC não aborda os pontos da mesma maneira que ambas as normas da ISO, ou seja, alguns pontos são atividades parciais das descritas nas normas. Um exemplo é a comparação do ponto 4 Contexto da organização, que tem como objetivos entender o contexto da organização, as necessidades e as expectativas das partes interessadas e determinar o escopo de um ISMS/ SGDA, com o modelo do DCC, cujo único ponto a ligar-se a este seria a participação e observação da comunidade, denotando a falta de observação dos outros pontos propostos pelas normas.

Outro ponto a ser comparado, quanto à completude de atividades é o ponto 5 Liderança, no qual aponta especificamente os papéis que devem ser realizados pelos líderes. O modelo do DCC não apresenta de forma clara a participação da liderança, apesar de no tópico de Curadoria e preservação apontar ações administrativas e estratégicas que devem ser realizadas, não se preocupa com as funções e responsabilidades a serem desempenhadas.

No geral, no que se refere à completude dos documentos, os documentos estão completos, possuindo ações estratégicas, gerenciais e operacionais. Apesar das normas ISO serem um pouco mais completas, isso se deve ao facto de seu âmbito de aplicação ser mais extenso do que do modelo do DCC.

7.4 Flexibilidade

O aspeto flexibilidade visa discorrer sobre o nível de adaptação dos documentos em relação à aplicabilidade com outros documentos. Em outras palavras, se os documentos podem ser aplicados sozinhos ou em conjunto.

O modelo do DCC, como discutido por Higgins (2008), é um modelo holístico, mais genérico do que exaustivo. A autora ainda aponta que este pode ser utilizado com outros modelos, esquemas e normas que o ajudem a granular mais as suas atividades. Sara Higgins (2009) ainda aponta que a utilização de outros documentos que auxiliem a implementação, assegurariam a continuidade do processo e manteriam íntegras as características da informação. Mais comumente a utilização de normas e esquemas que

auxiliem a representação descritiva da informação, como a utilização da ISAD(G) (*International Standard Archival Description (General)*), para a descrição de materiais arquivísticos e a AACR2 (*Anglo-American Cataloguing Rules, 2nd Edition*) para a catalogação de livros, ou o VRA Core, que auxilia a descrição de documentos de imagem, entre outros. No geral, o modelo do DCC é mais estratégico do que operacional, o que sugere a utilização de outras normas, para aplicação de padrões em todos os níveis.

Como apresentado no subcapítulo 4.2, a norma ISO/IEC 27001 vem de uma família que apresenta diversos tópicos na área da tecnologia da informação, desde o vocabulário, requisitos e definições para aplicação de ações de segurança da informação. Apesar da norma ser compreensível e possível de ser aplicada sozinha, uma aplicação em conjunto com outras normas da família ISO seria o cenário ideal, por exemplo no exposto na figura 4 com a implementação de um ISMS. Este é um processo deveras complexo constituído de diversas atividades que requerem a utilização de outras normas. Contudo, dependendo do contexto da organização, outras normas e esquemas podem ser utilizados para outros processos, não somente as normas da família ISO. Isso porque a norma ISO/IEC 27001 também é genérica e holística na descrição das atividades, o que permite a utilização de documentos secundários para guiar estas atividades. Assim como a norma ISO/IEC 27001, e como apresentado no subcapítulo 3.3, a norma ISO 30301 é altamente flexível e recomenda-se a utilização de outras normas e esquemas na sua aplicação.

Em síntese, os três documentos são altamente flexíveis, permitindo a utilização de outras normas e esquemas que venham auxiliar a descrição de atividades. De maneira geral, a estrutura deles são holística e estratégica, demandando, dessa forma, a utilização de documentos para a operacionalização das atividades.

7.5 Envolvimento da alta administração

O aspeto envolvimento da alta administração visa avaliar como essa é envolvida no processo de aplicabilidade dos sistemas de gestão, garantindo que as suas funções e responsabilidades estão claras e bem estruturadas.

Cabe apresentar que a importância da divisão de tarefas foi discutida por Max Weber (1947) ao explicar a Teoria da Burocracia. Segundo Chiavenato (2003, p. 262) citando o trabalho de Weber (1947), algumas das características da burocracia são:

- “Caráter legal das normas e regulamentos.

- Caráter formal das comunicações.
- Caráter racional e divisão do trabalho.
- Impessoalidade nas relações.
- Hierarquia de autoridade.
- Rotinas e procedimentos padronizados.
- Competência técnica e meritocracia.
- Especialização da administração.
- Profissionalização dos participantes.
- Completa previsibilidade do funcionamento"

A partir da utilização desta teoria administrativa, que é amplamente utilizada em diversas organizações, Chiavenato (2003, p. 266), ainda baseando-se no trabalho de Weber (1947), aponta algumas das vantagens da burocracia, a saber:

- "Racionalidade em relação ao alcance dos objetivos da organização.
- Precisão na definição do cargo e na operação, pelo conhecimento exato dos deveres.
- Rapidez nas decisões, pois cada um conhece o que deve ser feito e por quem e as ordens e papéis tramitam através de canais pré-estabelecidos.
- Uniformidade de rotinas e procedimentos que favorece a padronização, a redução de custos e erros, pois as rotinas são definidas por escrito."

Nota-se, portanto, que a utilização de modelos e normas, como exposto, são procedimentos básicos neste cenário. Com isso, há a necessidade de melhor estruturação de certos pontos, como o envolvimento da alta administração e a definição de funções e responsabilidades.

O modelo do DCC, como apresentado no ponto 7.3, não possui o tópico Liderança como em ambas as normas ISO. Efetivamente, as funções e responsabilidades da liderança não estão explícitas e claras, apresentando-se apenas algumas atividades que devem ser desenvolvidas em âmbito estratégico. Contudo, ambas as normas ISO apresentam as funções e atividades que devem ser desempenhadas pela alta administração. Neste caso, a liderança e comprometimento, as políticas a serem desenvolvidas e as funções e responsabilidades e autoridades organizacionais que devem ser desempenhadas pela alta administração. Uma melhor definição de papéis deve ser desenvolvida no modelo do DCC de maneira a assegurar melhor compreensão e evitar discrepâncias na aplicação do modelo.

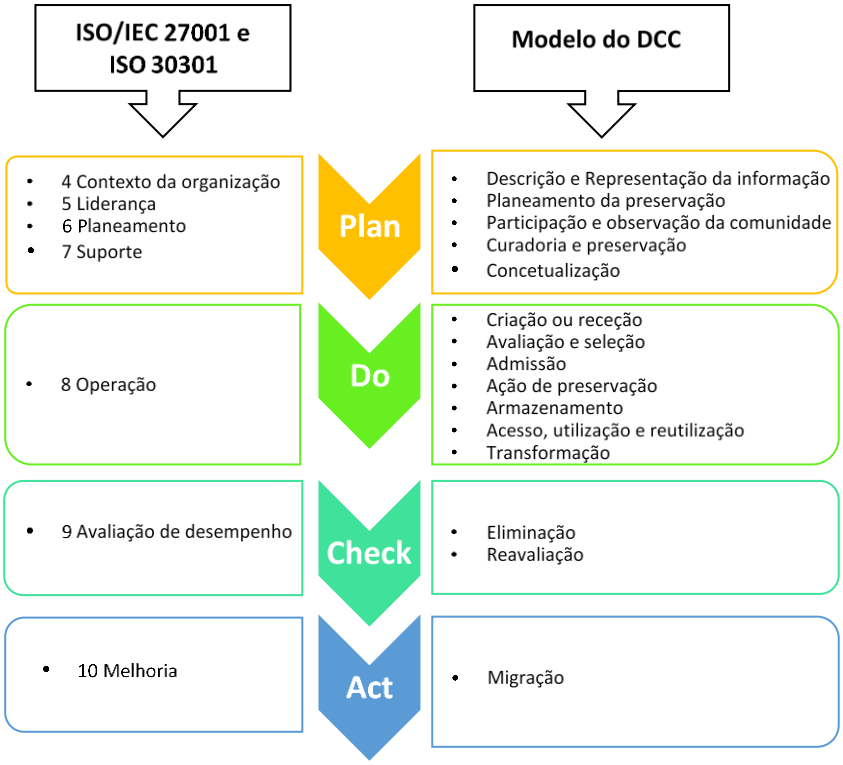
7.6 Continuidade do processo e melhoria

Este item visa avaliar como cada um dos documentos entende a continuidade do processo e as suas ações de melhoria.

A realização desta análise, embasou-se no processo do PDCA, de William Deming (ver capítulo 5). Este método de melhoria contínua de processos baseia-se em quatro passos (*Plan, Do, Check e Act)* de forma que estes são realizados em etapas, aplicando-se testes de melhoria, preferencialmente em pequena escala, analisando-se os resultados e, caso bem-sucedidos, aplicando-os em larga escala.

Como já apresentado, a norma ISO/IEC 27001 utiliza este método na implementação de um ISMS, de maneira que qualquer melhoria ou aplicação deverá ser testada e conferida. A vantagem da aplicação deste ciclo é que após a etapa *Act* há um reinício do processo, garantindo assim a correção de eventuais falhas. Assim como a ISO/IEC 27001, a norma ISO 30301 também é baseada no modelo do PDCA, ela apresenta a sua estrutura, na introdução da norma. O modelo do DCC, todavia, apesar de não explicitamente, apresenta também as etapas desta metodologia. A figura 11 abaixo apresenta as atividades de ambas as normas e do modelo do DCC divididos segundo o processo do PDCA.

Figura 11 - PDCA na S.I, GI e CI.



Fonte: elaboração própria.

Como observado, as atividades dos processos descritos em ambos documentos encaixam- se a este método. Outro exemplo é referente às alterações realizadas em ambos documentos. No caso da norma ISO/IEC 27001, a sua primeira versão foi lançada em 2005 e após mudanças em certos tópicos, como por exemplo a retirada do modelo do PDCA do tópico abordagem de processos, foi revista e relançada em 2013. Em 2019 houve nova revisão confirmada, entretanto a versão de 2013 ainda se mantém atual. Cabe mencionar que dois documentos com alterações à norma foram lançados (um em 2014 e um em 2015) apontando melhorias ao processo. Assim como a norma ISO 30301 que foi lançada em 2011 e após revisão, sofreu pequenas alterações e foi relançada em 2019.

O modelo do DCC, da mesma forma, também sofreu mudanças e melhorias, como apresentado nos artigos de Higgins (2007, 2008). Em 2007 a autora apresentou o modelo preliminar e lançou-o para consulta pública até fevereiro de 2008. Após este período foram feitas correções e melhorias, cujo resultado foi apresentado no artigo da mesma em junho de 2008. Atualmente, o DCC orienta no seu *website* que sejam enviadas quaisquer sugestões de melhoria para que, após verificações, possam ser implementadas.

Em síntese, os documentos apresentam as etapas para a continuidade de processos e melhoria contínua. Estes apresentam factos que compreendem a necessidade de se fazer correções quando necessário e proveem as ferramentas para tal.

Para concluir a análise comparativa, vale ressaltar que devido à particularidade de cada área, a aplicação de cada um dos processos é direcionada. Dessa forma, para se realizar esta análise, pontos muito particulares e exclusivos de cada área, como por exemplo análise de risco (S.I) e a preservação de documentos (modelo DCC), foram desconsiderados. De forma geral, esta análise foi realizada de maneira mais abrangente, tentando englobar características mais holísticas de cada documento.

Isto posto, nota-se que o modelo do DCC é mais granulado em relação à descrição de processos operacionais. Já em ambas as normas da ISO, essa granularidade é encontrada no documento anexo, o qual possui maior descrição de diversas atividades do processo. De forma geral, a norma ISO/IEC 27001 e a norma ISO 30301 são melhor estruturadas, melhor subdivididas, mais complexas e possuem melhor delimitação do envolvimento da alta administração. Porém, os três documentos analisados possuem uma

linguagem clara e consistente, estão completas em relação às ações estratégicas, gerenciais e operacionais, possuem estrutura holística e estratégica e possuem um processo de melhoria bem desenvolvido.

8. Proposta de alinhamento entre os processos

Após a realização da análise comparativa, compete-se à procedência do alinhamento dos documentos de maneira a poder otimizar os processos da GCI com os da SI, tornando-os mais eficientes e eficazes e desenvolver um modelo destes processos, considerando os pontos positivos e negativos supramencionados.

Primeiramente, para clarificar a junção dos processos, criou-se a figura 12, a qual demonstra quais as atividades que seriam similares, ou parcialmente similares, nos documentos. Salienta-se que para este alinhamento, desconsiderou-se os quatro primeiros tópicos descritos nas normas ISO/IEC 27001 e ISO 30301 (do tópico 0 ao 3), devido a serem introdutórios e não propriamente a apresentação das atividades do processo. Em segundo lugar, cabe frisar que devido à melhor estrutura dos processos de SI e GI as ações do modelo do DCC foram incorporadas às seções descritas nas normas. A seguir explanar-se-á este alinhamento e as conexões estabelecidas.

Figura 12 - *Alinhamento entre os processos de SI e GI com o modelo do DCC.*

Fonte: Elaboração própria.

A ação Participação e observação da comunidade liga-se à seção 4 Contexto da organização devido este ser um dos pontos abordados neste tema, como apontado no subcapítulo 7.3. Retomando que a seção "4 Contexto da organização", como descrito nas norma ISO/IEC 27001 e ISO 30301, possui mais tópicos que devem ser apreendidos para a definição do contexto e dos requisitos relativos ao entendimento da organização, como o "4.1 Entendendo a organização e o seu contexto" (e os sub subtópicos da ISO 30301), o "4.3 Determinando o âmbito do sistema de gerenciamento de segurança da informação/ documentos de arquivo" e o "4.4 Sistema de gestão de segurança da informação/ documentos de arquivo". Todavia, dado as ações "4.2 Compreendendo as necessidades e expectativas das partes interessadas" e a "Participação e observação da comunidade", possuírem o mesmo objetivo, elas foram integradas num mesmo ponto. À vista disto, para o desenvolvimento sugere-se a adição dos seguintes tópicos, a saber:

- Contexto da organização
    - Entendendo a organização e o seu contexto
        - Geral
        - Requisitos dos documentos
    - Compreendendo as necessidades e expectativas das partes interessadas.
    - Determinando o âmbito do sistema de gerenciamento de segurança da informação/ documentos de arquivo
    - Sistema de gerenciamento de segurança da informação/ documentos de arquivo

A ação Curadoria e preservação deveria estar englobada na seção 5 Liderança de ambas as normas ISO, isto porque a curadoria e preservação está relacionada às ações administrativas e de gestão que devem ser realizadas durante a utilização do modelo, sendo estas a serem desenvolvidas pela liderança. Todavia, esta atividade não representa o processo inteiro descrito nesta seção, visto que outras ações e funções que devem ser desempenhadas pela alta administração não estão descritas, como as apontadas nas subseções "5.1 Liderança e compromisso", "5.2 Política" e "5.3 Funções,

responsabilidades e autoridades organizacionais". Assim, sugere-se a incorporação da ação Curadoria e preservação às da seção "5 Liderança", a saber:

- Liderança
  - Liderança e compromisso
  - Política
  - Funções, responsabilidades e autoridades
  - Ações de curadoria e preservação

As ações Planeamento da preservação e Concetualização interligam-se à seção 6 Planeamento das normas ISO devido a ambos os tópicos serem voltados à parte de delineação de ações e planeamento. Entretanto, as subseções das normas são demasiadamente particulares à suas próprias áreas, de modo que as ações dispostas no modelo do DCC foram incluídas de maneira separada, da seguinte forma:

- Planeamento
  - Ações para lidar com riscos e oportunidades
  - Objetivos da segurança da informação/ dos documentos e planeamento para alcançá-los
  - Planeamento da preservação
  - Concetualização

A ação Descrição e Representação da informação está associada à seção 7 Suporte, pois este apresenta requisitos relativos aos suportes utilizados na implementação de um ISMS/ SGDA. As ações Criação ou receção, Avaliação e seleção, Admissão, Ação de preservação, Armazenamento, Acesso, utilização e reutilização apesar de estarem associadas a processos operacionais, na norma ISO 30301 estes são incluídos na seção 7, dessa forma, devido a maior granularidade dos processos no modelo do DCC, decidiu-se por manter a divisão do DCC em detrimento da divisão da norma ISO 30301. As outras subseções que apresentam a determinação dos recursos, competências, consciência dos procedimentos e comunicação foram mantidos, como especificado a seguir:

- Suporte
  - Recursos
  - Competência

- Consciência
- Comunicação
- Descrição e Representação da informação
- Informação documentada
    - Criação ou receção
    - Avaliação e seleção
    - Admissão
    - Ação de preservação
    - Armazenamento
    - Acesso, utilização e reutilização
    - Transformação

O modelo do DCC carece de ações que se alinhem à seção 8 Operação das normas. Esta seção descreve o planeamento de procedimentos operacionais, e devido à particularidade de cada área, possuem atividades distintas, mas que para a GCI entendeu-se que se complementam. Desta forma, decidiu-se manter os processos descritos na norma ISO 30301 e na norma ISO/IEC 27001:

- Operação
    - Planeamento e controlo operacional
    - Determinando arquivos a serem criados
    - Desenho e implementação de processos, controlos e sistemas de arquivos
    - Avaliação de risco à segurança da informação
    - Tratamento de riscos à segurança da informação

A ação Reavaliação liga-se à seção 9 Avaliação de desempenho dado que ambos procuram avaliar possíveis problemas existentes no processo. Esta seção apresenta a revisão de seu próprio modelo, o que é um fator de melhoria contínua de processo, como os descritos nas subseções "9.2 Auditoria interna" e "9.3 Revisão da administração". Apesar da seção "9.1 Monitoramento, medição, análise e avaliação" e da ação "Reavaliação" serem muito semelhantes, decidiu-se separá-las para que os seus objetivos ficassem mais granulados. Desta forma à seção 9.1 tratar-se-ia de análise de *performance*,

enquanto a ação “Reavaliação”, de análise da documentação. Destarte, este tópico ficaria disposto da seguinte forma:

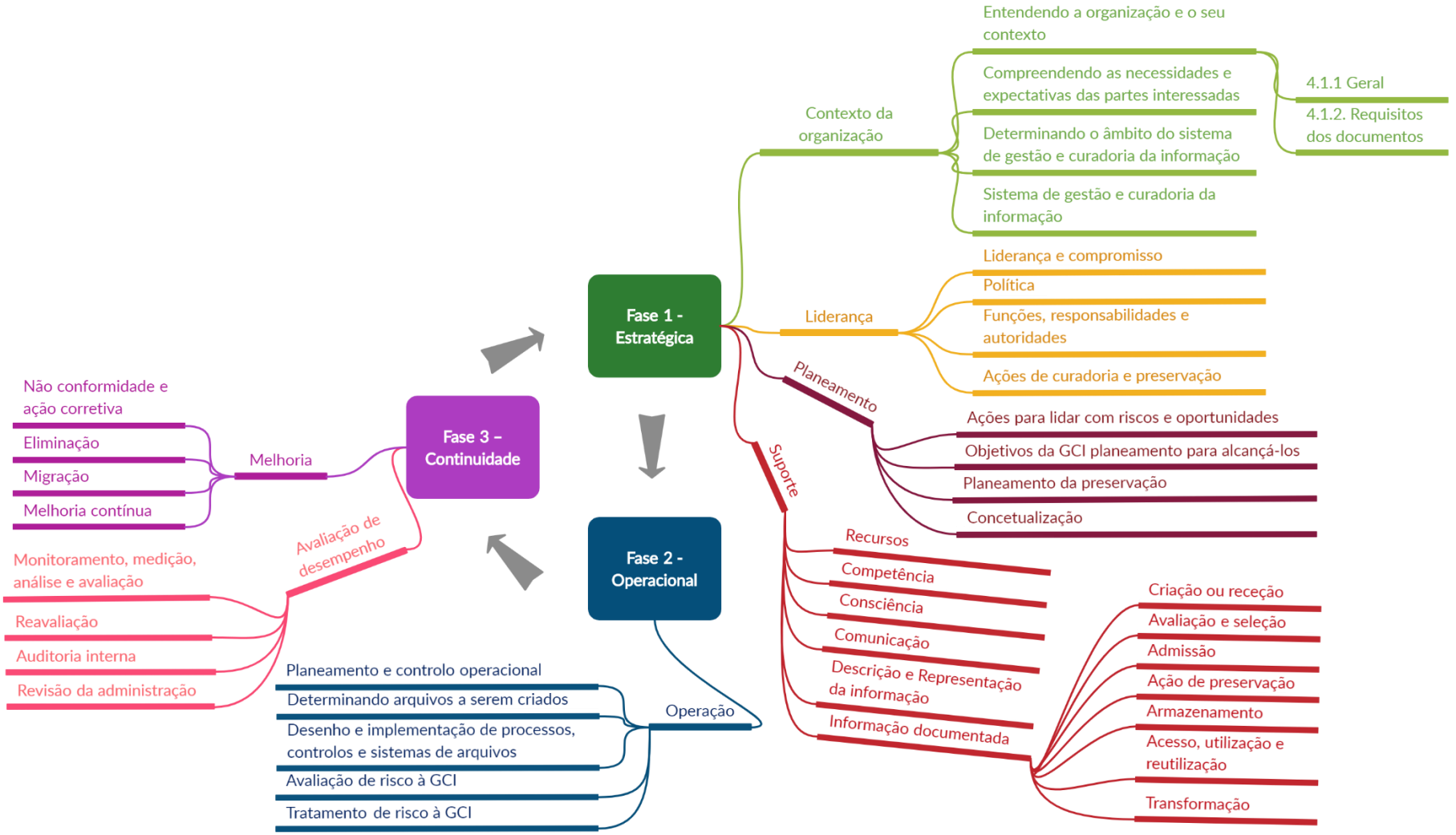
- Avaliação de desempenho
  - Monitoramento, medição, análise e avaliação
  - Reavaliação
  - Auditoria interna
  - Revisão da administração

As ações Eliminação e Migração vinculam-se à seção 10 Melhoria. Ambos os tópicos do modelo do DCC podem ser descritos como similares à seção “10.1 Não conformidade e ação corretiva” das normas da ISO. Contudo, devido à importância destes itens para a GCI e para a SI, decidiu-se mantê-los todos. Assim como o item melhoria contínua, que visa a parte *Act* do PDCA, que também perdurou, ficando exposto da seguinte forma:

- Melhoria
  - Não conformidade e ação corretiva
  - Eliminação
  - Migração
  - Melhoria contínua.

Concluindo o alinhamento dos processos e considerando a pertinência de cada item à GCI e a SI e a agregação de valor aos processos, foi possível desenvolver um modelo para os exemplificar (figura 13). Este modelo desenvolvido apresenta o processo de GCI baseando-se no alinhamento entre os processos das três áreas em estudo, dividindo-se em três fases: estratégica, operacional e continuidade.

Figura 13 - *Modelo de processos alinhados.*



Fonte: Elaboração própria.

A partir das definições fornecidas nas normas ISO/IEC 27001 e ISO 30301 e das descrições das tabelas do modelo do DCC foi possível explicitar as fases do processo da GCI.

Fase 1 – Estratégica

1. **Contexto da organização:** Definição dos requisitos para o entendimento de assuntos externos e internos, partes interessadas, expectativa da organização e a definição do escopo da GCI.
   1.1. **Entendendo a organização e o seu contexto:** Requisitos para o entendimento da organização no contexto interno e externo.
      1.1.1. **Geral:** Apresenta informações gerais sobre os requisitos da organização e seu contexto.
      1.1.2. **Requisitos dos documentos:** Determina os requisitos de análise dos documentos.
   1.2. **Compreendendo as necessidades e expectativas das partes interessadas:** Determine as partes interessadas e as expectativas da organização. Acompanhe as atividades apropriadas da comunidade e participe do desenvolvimento de padrões, ferramentas e *software* adequados
   1.3. **Determinando o âmbito do sistema de gestão e curadoria da informação:** Determine a aplicação e limites da GCI.
   1.4. **Sistema de gestão e curadoria da informação:** Entenda as etapas que devem ser seguidas e mantidas pela organização, ou seja, um processo contínuo.
2. **Liderança:** Determina o envolvimento e tarefas a serem desenvolvidas pelos líderes.
   2.1. **Liderança e compromisso:** Aponte o envolvimento dos líderes e os seus papéis quanto às ações de curadoria e preservação e aplicabilidade da GCI.
   2.2. **Política:** Estabeleça de uma política de segurança de informação.
   2.3. **Funções, responsabilidades e autoridades:** Determine as funções, responsabilidades e autoridades quanto à aplicabilidade da GCI.
   2.4. **Ações de curadoria e preservação:** Estabeleça uma política que apresente ações de curadoria e preservação, visando a longevidade e utilização dos materiais.
3. **Planeamento:** Planeamento das etapas relacionadas ao desenvolvimento de ações e métodos para a preservação.

3.1. **Ações para lidar com riscos e oportunidades:** Determine as ações a serem desenvolvidas em relação à avaliação e tratamento do risco.

3.2. **Objetivos da GCI e planeamento para alcançá-los:** Determine as etapas a serem realizadas para a implementação dos objetivos da GCI.

3.3. **Planeamento da preservação:** Planeie a preservação durante todo o ciclo de vida da curadoria de material digital. Isso inclui planos para gestão e administração de todas as ações do ciclo de vida de curadoria.

3.4. **Concetualização:** Conceba e planeie a criação de dados, incluindo o método de captura e opções de armazenamento.

4. **Suporte:** Requisitos relativos aos suportes necessários na implementação da GCI.

4.1. **Recursos:** Determine os recursos necessários.

4.2. **Competência:** Determine as competências necessárias.

4.3. **Consciência:** Apresente os documentos, procedimentos e outros itens que devem ser apresentados aos envolvidos na GCI.

4.4. **Comunicação:** Determine o quê, quando, como e quem deve ser comunicado sobre os processos da GCI

4.5. **Descrição e Representação da informação:** Atribua metadados administrativos, descritivos, técnicos, estruturais e de preservação, usando padrões adequados, para garantir uma descrição e controlo adequados a longo prazo. Recolher e atribuir a representação da informação necessárias para entender e apresentar o material digital e os metadados associados.

4.6. **Informação documentada:** Determina formas de lidar com a informação documentada, desde a criação, atualização, controlo, armazenamento, entre outros.

4.6.1. **Criação ou receção:** Crie dados, incluindo metadados administrativos, descritivos, estruturais e técnicos. Os metadados de preservação podem também ser adicionados no momento da criação. Receber dados, de acordo com as políticas de recolha documentadas, de criadores de dados, outros arquivos, repositórios ou centros de processamento de dados e, se necessário, atribuir metadados apropriados.

4.6.2. **Avaliação e seleção:** Avalie e selecione os dados para curadoria e preservação a longo prazo. Seguir as orientações, políticas ou requisitos legais documentados.

4.6.3. **Admissão:** Transfira dados para um arquivo, repositório, centro de processamento de dados ou para outro custodiante. Seguir as orientações, políticas ou requisitos legais documentados.

4.6.4. **Ação de preservação:** Realize ações para garantir a preservação e retenção a longo prazo da natureza autorizada dos dados. As ações de preservação devem garantir que os dados permaneçam autênticos, confiáveis e utilizáveis, mantendo a sua integridade. As ações incluem a limpeza, a validação, a designação de metadados de preservação, a designação de informações de representação e a garantia de estruturas de dados ou formatos de arquivo aceitáveis.

4.6.5. **Armazenamento:** Armazene os dados de forma segura, seguindo os padrões relevantes.

4.6.6. **Acesso, utilização e reutilização:** Garanta que os dados estejam acessíveis diariamente, tanto para utilizadores designados quanto para reutilizadores. Isto pode ser na forma de informações publicadas publicamente disponíveis. Controlos de acesso e procedimentos de autenticação robustos podem ser aplicáveis.

4.6.7. **Transformação:** Crie novos dados a partir do original, por exemplo, pela migração para um formato diferente ou criando um subconjunto, por seleção ou consulta, para criar novos resultados derivados, talvez para publicação

Fase 2 – Operacional

5. **Operação:** Apresenta os procedimentos operacionais para atingir a GCI.
   5.1. **Planeamento e controlo operacional:** Requerimentos para o planeamento e implementação do controlo operacional.
   5.2. **Determinando arquivos a serem criados:** Determina a criação da documentação de processos.
   5.3. **Desenho e implementação de processos, controlos e sistemas de arquivos:** Desenvolvimento e implementação dos processos de documento.
   5.4. **Avaliação de risco à GCI:** Determine a execução da avaliação de risco.
   5.5. **Tratamento de riscos à GCI:** Implemente o plano de tratamento de risco à GCI.

Fase 3 – Continuidade

6. **Avaliação de desempenho:** Avaliação e monitoramento dos processos da GCI.
   6.1. **Monitoramento, medição, análise e avaliação:** Determina o quê, quem, quando e como deve ser monitorado, medido, analisado e avaliado o desempenho da GCI.
   6.2. **Reavaliação:** Retorne dados que falhem nos procedimentos de validação para avaliação e re-seleção posterior.
   6.3. **Auditoria interna:** Apresente os aspetos para a auditoria da GCI.
   6.4. **Revisão da administração:** Determine a revisão dos processos da GCI pelos gestores.
7. **Melhoria:** Apresenta ações de melhoria para os processos.
   7.1. **Não conformidade e ação corretiva:** Determine ações quanto às atividades que apresentam não conformidade e ações corretivas.
   7.2. **Eliminação:** Descarte os dados que não foram selecionados para curadoria e preservação a longo prazo, de acordo com políticas, orientações ou requisitos legais documentados. Normalmente, os dados podem ser transferidos para outro arquivo, repositório, centro de processamento de dados ou para outro custodiante. Em alguns casos, os dados são destruídos. A natureza dos dados pode, por razões legais, exigir destruição segura.
   7.3. **Migração:** Migre dados para um formato diferente. Isso pode ser feito de acordo com o ambiente de armazenamento ou para garantir a imunidade dos dados à obsolescência de *hardware* ou *software*.
   7.4. **Melhoria contínua:** Determine a continuidade da melhoria dos processos impostos no modelo.

Este modelo apresenta a integração dos processos de GCI e SI subdivididos em três fases de aplicação: estratégica, operacional e contínua. Esta subdivisão foi pensada utilizando a proposta do modelo PDCA, contudo as fases *Check* e *Act* foram integradas numa fase única, devido aos seus processos serem muitas vezes realizados em simultâneo e/ou de forma conjunta, nos processos do GCI, por exemplo, as ações de Migração e Eliminação. Outro motivo da junção de ambas fases, é devido à possibilidade destes processos serem entendidos como gerenciais (vide subcapítulo 7.3). Apesar de todo o modelo do PDCA ser cíclico de maneira a garantir a melhoria contínua dos processos, as

fases *Check* e *Act* estão voltadas à análise da implementação da melhoria, visando a continuidade dos processos. Em razão disto, toda a estrutura do modelo foi feita seguindo a mesma lógica. Nota-se que esta também é a estrutura da norma ISO 30301 e da norma ISO/IEC 27001, como discutidos nos subcapítulos 3.3 e 4.3 e devido a serem claras, completas e sequenciais (vide subcapítulo 7.1) preferiu-se pela seleção destas, do que a anteriormente descrita no modelo do DCC.

Quanto à linguagem utilizada para a descrição das atividades, cabe mencionar que redobrada atenção foi tida ao desenvolver a terminologia das seções descritivas, pois esta tinha como objetivo manter a estrutura dos documentos analisados, integrando-os e mantendo as peculiaridades da sua expressividade. Desta forma, manteve-se a utilização sintáxica como descrita no modelo do DCC (subcapítulo 7.2): forma padrão do verbo, orações imperativas afirmativas e descritivas. Outro ponto importante mencionar é relativo ao conteúdo do campo descrição, no qual é possível observar diversas semelhanças entre os documentos alinhados. De facto, a descrição é praticamente idêntica às dos documentos nos quais foram baseados, sofrendo mínimas alterações somente quando o âmbito de aplicação exigisse. Isso se deve ao objetivo proposto por esta pesquisa: fazer um alinhamento entre os processos já existentes em ambas áreas.

Para o desenvolvimento deste modelo, considerou-se também uma das características mais importantes que foi destacada no subcapítulo 7.4, a flexibilidade. Devido a ambos os modelos serem altamente flexíveis, permitindo a utilização de outras normas e esquemas, evitou-se retirar esta característica. Em outras palavras, o modelo dos processos de SI e GCI contínua sendo estratégico e holístico, ainda demandando a utilização de outras documentações que auxiliem operações secundárias, como descrito na atividade Planeamento.

Não obstante uma das atividades que sofreu maior alteração em relação ao modelo anterior foi referente à adição das ações explícitas da alta administração, como supramencionado. De maneira a garantir a melhoria da eficácia e eficiência dos processos, a descrição das atividades deve ser clara e unívoca, como apresentado na Teoria da Burocracia de Weber (1947). Esta racionalização nesta etapa do processo reduz futuras falhas e reduz custos no processo como um todo.

Deste modo, após uma análise comparativa dos processos por meio de aspetos selecionados, distinguiu-se pontos positivos e negativos nos processos de GCI e SI. Foi possível determinar pontos de sinergia entre eles apesar do domínio de aplicação destes

serem distintos e em virtude dos factos mencionados, perfaz-se que a hipótese 1 foi corroborada, ou seja, ambas áreas possuem processos que se alinham.

No que concerne à hipótese 2, pode-se constatar que esta também foi corroborada. Visto que uma norma bem estruturada deve ser capaz de melhorar a *performance* dos processos de uma área, como discutido no subcapítulo 7.1. Ademais, apesar de o modelo do DCC ter como foco principal a curadoria da informação, muitos tópicos relativos à gestão estão indeterminados, como por exemplo, os relativos à liderança, como referido no subcapítulo 7.5, sendo estes apresentados somente nas normas ISO. Pela observação dos aspetos analisados pode-se concluir que há uma melhoria da aplicabilidade da GCI devido a estruturação de normas, baseando-se nos processos das suas áreas de estudo oriundas.

A hipótese 3, cujo prognóstico previa a existência de uma relação positiva em termos de melhoria na eficácia e eficiência quando a GCI e a SI são aplicadas em conjunto, foi parcialmente provada. Isto porque, como observado, na teoria existem muitos pontos de sinergia entre os processos de ambas as áreas, como apontado no modelo desenvolvido (figura 13). Devido à estrutura deste modelo ser baseado nos processos descritos nas normas ISO/IEC 27001 e ISO 30301, que apresentam melhores condições de aplicabilidade, evidentemente, melhoraria a eficiência e eficácia quando aplicado em organizações. Contudo, para comprovar a aplicação prática desta hipótese, seria necessário a realização de um caso de estudo, no qual se obteria dados suficientes para a validação ou não da mesma.

Em suma, foi possível realizar o alinhamento dos processos da SI e os da GCI de maneira a torná-los mais eficazes e eficientes ao serem aplicados numa organização. E a partir deste alinhamento, foi possível desenvolver um modelo da GCI, tornando os processos visualmente mais organizados e mantendo a sua expressividade, possibilitando a interligação das três áreas de forma holística.

9. Conclusões

Este trabalho assumiu como objetivo analisar de que modo diferem ou se assemelham os objetivos, princípios, processos, métodos e técnicas por um lado da GCI e por outro lado os da SI, além de identificar oportunidades de sinergias que possam levar a uma melhor eficiência e eficácia na sua aplicação.

Para este fim, escolheu-se o método de pesquisa exploratório e comparativo. Desta forma, procedeu-se primeiramente com a revisão da literatura de ambas as áreas, apresentando os seus principais conceitos, objetivos, processos e métodos de maneira a clarificá-los e compreendê-los. Em seguida, realizou-se uma análise comparativa de forma a apontar os pontos positivos e os pontos que carecem de melhoria e assim, prosseguir a discussão para equiparar ambas as áreas.

Para auxiliar o desenvolvimento da pesquisa, conjecturou-se três hipóteses que atuaram como ponto de partida para explorar estes temas. Após a realização da análise foi possível verificar que as hipóteses 1 e 2 foram completamente corroboradas, enquanto a terceira, foi apenas parcialmente.

Assim, uma das conclusões possíveis de inferir desta pesquisa é que é possível realizar a aplicação de ambos processos em conjunto e, na verdade, uma integração beneficiaria a organização, pois aumentaria a granularidade de certos processos, mantendo ainda a sua característica holística. Em virtude do que foi mencionado sobre o ciclo do PDCA e o seu processo de melhoria contínua, também foi possível constatar que ambos ao processos contêm esta característica de forma intrínseca e, com o alinhamento de ambos, foi possível mantê-la.

É importante salientar que um dos resultados mais relevantes desta pesquisa foi em relação à organização da informação de uma forma mais estruturada, principalmente no tocante aos processos da GCI. Como apresentado na figura 13, a originalidade na junção e organização da informação agrega valor e auxilia o entendimento e discriminação dos processos.

Este estudo apresenta algumas limitações, nomeadamente ao nível prático de aplicabilidade dos processos. Como supramencionado, apesar de na teoria ser possível identificar e indicar os pontos de sinergia entre os processos, na prática, não foi possível obter dados necessários para a comprovação de tal. Primeiramente, porque este sairia do âmbito da metodologia proposta neste trabalho. Em segundo lugar, porque, a nível de

recolha dos dados, quando relativos à segurança da informação, deve-se considerar a questão da privacidade dos dados e como a maior parte destes são sigilosos e as organizações, no geral, não estão dispostas a ceder tais dados para pesquisa.

Outra limitação é em relação aos próprios processos da área de GCI, que por não serem tão bem estruturados e identificáveis quanto os da SI, acabam por ser adaptados, muitas vezes de outras áreas. Esta limitação deve-se ao facto que a GCI ainda é uma área nova, que necessita de uma maior densidade, mas que, segundo Higgins (2018), vai ocorrer ao longo do ciclo de *feedback* entre a academia e o mercado.

Apesar das limitações identificadas, e de outras que podem ser apontadas, considera-se que o estudo realizado permitiu compreender os processos de ambas as áreas e contribuir para o desenvolvimento e melhoria das práticas da área da GCI. Além de ressaltar a necessidade do mercado em relação à ambivalência de competências, agregação de valor, tratamento da informação, consciencialização das necessidades dos interessados e visualização holística dos processos que a GCI inclui.

Em vista dos argumentos apresentados, seria interessante o desenvolvimento de trabalhos futuros nos quais a aplicação destes processos pudessem ser observado, levando em consideração todas as dificuldades que estas implicam, como a gestão da privacidade dos dados, a utilização do RGPD e outras normas e regulamentos relativos ao tratamento, utilização, armazenamento e uso de informações. Além de estudos de uso dos processos de SI e GCI aplicados em conjunto e o seu desempenho no controlo e utilização das informações em momentos de crise, como por exemplo, durante a operação de trabalho remoto que ocorreu em larga escala devido à pandemia da COVID-19. Ademais trabalhos que aprofundem, sugiram e estabeleçam processos e práticas melhor desenvolvidos e estruturados da GCI seriam de grande auxílio à área, tanto académica quanto profissional.

Referências

Abbott, D. (2008). *What is Digital Curation?* DCC Briefing Papers: Introduction to Curation. http://www.dcc.ac.uk/resources/briefing-papers/introduction-curation/what-digital-curation

ABNT. (2016). *ABNT NBR ISO 30301:2016 Informação e documentação — Sistemas de gestão de documentos de arquivo — Requisitos*. https://fatecsenai.com.br/arquivos/30301-Informacao-e-documentacao-Sistemas-de-Gestao-de-Documentos-de-arquivo-Requisitos.pdf

About the ISO27k standards. (2020). iso27001security. https://www.iso27001security.com/html/iso27000.html

Aitken, R. (2018). Global Information Security Spending To Exceed $124B In 2019, Privacy Concerns Driving Demand. *Forbes*. https://www.forbes.com/sites/rogeraitken/2018/08/19/global-information-security-spending-to-exceed-124b-in-2019-privacy-concerns-driving-demand/#7032a5807112

Anthony, R. N. (1965). *Planning and Control: A Framework for Analysis.* Harvard University Press.

Ball, A. (2012). *Review of Data Management Lifecycle Models*. University of Bath. https://purehost.bath.ac.uk/ws/portalfiles/portal/206543/redm1rep120110ab10.pdf

Barata, P. J. S., & Ochôa, P. (2015). Profissionais de Informação-Documentação a caminho da invisibilidade: Uma reflexão a partir da análise de cargos de direção intermédia na Administração Central do Estado. *Cadernos BAD*, *1*(1), 7–22. https://www.bad.pt/publicacoes/index.php/cadernos/article/view/1152

Baskarada, S., & Koronios, A. (2013). Data, Information, Knowledge, Wisdom (DIKW): A Semiotic Theoretical and Empirical Exploration of the Hierarchy and its Quality Dimension. *Australasian Journal of Information Systems*, *18*(1), 5–24. https://doi.org/10.3127/ajis.v18i1.748

Bawden, D., & Robinson, L. (2012). *Introduction to Information Science*. Facet Publishing.

BBC. (2019). Cyber-attacks on UK firms «jump» in 2019. *BBC News*. https://www.bbc.com/news/business-48017943

Benjamin Martz Jr., Wm., & Shepherd, M. M. (2003). Testing for the Transfer of Tacit Knowledge: Making a Case for Implicit Learning. *Decision Sciences Journal of Innovative Education*, *1*(1), 41–56. https://doi.org/10.1111/1540-5915.00004

Bottle, R. T. (2003). Information Science. Em J. Feather & P. Sturges, *International Encyclopedia of Information and Library Science* (2.ª ed.). Routledge.

Bryman, A. (2012). *Social research methods* (4th ed.). Oxford University Press.

Burke, P. (2003). *Uma história social do conhecimento: De Gutenberg a Diderot.* Jorge Zahar Ed.

Campos, A. (2014). *Sistema de segurança da informação: Controlando os riscos.* (3.ª ed.). Visual Books.

Capurro, R., & Hjørland, B. (2003). The concept of information. *Annual Review of Information Science and Technology*, *37*(1), 343–411. https://doi.org/10.1002/aris.1440370109

Carretero Gomez, S., Vuorikari, R., & Punie, Y. (2017). *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. EU Science hub.

https://publications.jrc.ec.europa.eu/repository/bitstream/JRC106281/web-digcomp2.1pdf_(online).pdf

Castells, M. (1999). *A sociedade em rede* (6ªed, Vol. 1). Paz e Terra.

Centobelli, P., Cerchione, R., & Esposito, E. (2018). Aligning enterprise knowledge and knowledge management systems to improve efficiency and effectiveness performance: A three-dimensional Fuzzy-based decision support system. *Expert Systems with Applications*, *91*, 107–126. https://doi.org/10.1016/j.eswa.2017.08.032

Chappelow, J. (2020). *Trailing Definition*. Investopedia. https://www.investopedia.com/terms/t/trailing.asp

Chen, J. (2018). *Leading Indicator*. Investopedia. https://www.investopedia.com/terms/l/leadingindicator.asp

Chen, Y.-N., Chen, S.-J., & Lin, S. C. (2003). A metadata lifecycle model for digital libraries: Methodology and application for an evidence-based approach to library research. *Documents in Information Science, Working Papers Series.* World Library and Information Congress: 69th IFLA General Conference and Council, Berlim. https://archive.ifla.org/IV/ifla69/papers/141e-Chen_Chen_Lin.pdf

Chiavenato, I. (2003). *Introdução à teoria geral da administração: Uma visão abrangente da moderna administração das organizações* (7. ed.). Elsevier.

Creswell, J. R. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage Publications, Inc.

Dantas, M. L. (2011). *Segurança da informação: Uma abordagem focada em gestão de riscos*. Livro Rápido.

Davenport, T., & Grover, V. (2001). General Perspectives on Knowledge Management: Fostering a Research Agenda. *Journal of Management Information Systems*, *18*(1), 5–22. https://doi.org/10.1080/07421222.2001.11045672

De Mauro, A., Greco, M., & Grimaldi, M. (2014). *What is Big Data? A Consensual Definition and a Review of Key Research Topics*. 4th International Conference on Integrated Information, Madrid. https://doi.org/10.13140/2.1.2341.5048

Detlor, B. (2010). Information management. *International Journal of Information Management*, *30*(2), 103–108. https://doi.org/10.1016/j.ijinfomgt.2009.12.001

Digital Curation Centre. (2020). *DCC Curation Lifecycle Model | Digital Curation Centre*. Digital Curation Centre. http://www.dcc.ac.uk/resources/curation-lifecycle-model

Dukes, P. (2006). *Making the most of our data: MRC's data sharing & preservation initiative.* Medical Research Council. http://www.rin.ac.uk/system/files/attachments/Peter%20Dukes%20v2.pdf

EUR-lex. (2020). *Estratégia para o Mercado Único Digital – Revisão intercalar—EUR-Lex*. EUR-lex. https://eur-lex.europa.eu/content/news/digital_market.html?locale=pt

Faundeen, J. L., Burley, T. E., Carlino, J. A., Govoni, D. L., Henkel, H. S., Holl, S. L., Hutchison, V. B., Martín, E., Montgomery, E. T., Ladino, C. C., Tessler, S., & Zolly, L. S. (2014). *The United States Geological Survey Science Data Lifecycle Model* (Open-File Report N. 2013–1265; Open-File Report). U.S. Department of the Interior. https://pubs.usgs.gov/of/2013/1265/pdf/of2013-1265.pdf

Goodman, E. C. (1994). Records management as an information management discipline—A case study from SmithKline Beecham pharmaceuticals.

International Journal of Information Management, *14*(2), 134–143. https://doi.org/10.1016/0268-4012(94)90032-9

Gorry, G. A., & Morton, M. S. S. (1989). A Framework for Management Information Systems. *Sloan Management Review*, *13*, 21–39. https://web.archive.org/web/20030614170155/http://mis.njit.edu/ullman/cis465/Articles/gorry.pdf

Gouveia, L. B. (2016). *Gestão da Segurança da Informação: Conceitos básicos e introdução ao tema*. https://bdigital.ufp.pt/bitstream/10284/5954/1/securv1_1_mar2016.pdf

Gu, F., & Wang, W. (2005). Intangible assets, information complexity, and analysts' earnings forecasts. *Journal of Business Finance & Accounting*, *32*(9–10), 1673–1702. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.0306-686X.2005.00644.x

Henriques, R. (2017). Mestrado «Gestão e Curadoria da Informação». *Encontro Curadoria Digital – Estratégias e experiências: atas*, 44–47. https://repositorio.ual.pt/bitstream/11144/3708/3/Ebook%20Encontro%20Curadoria%20Digital%200509.pdf

Higgins, S. (2007). Draft DCC Curation Lifecycle Model. *International Journal of Digital Curation*, *2*(2), 82–87. https://doi.org/10.2218/ijdc.v2i2.30

Higgins, S. (2008). The DCC Curation Lifecycle Model. *International Journal of Digital Curation*, *3*(1), 134–140. https://doi.org/10.2218/ijdc.v3i1.48

Higgins, S. (2009). DCC DIFFUSE Standards Frameworks: A Standards Path through the Curation Lifecycle. *The International Journal of Digital Curation*, *2*(4), 60–67. http://www.ijdc.net/article/view/118

Higgins, S. (2011). Digital Curation:The Emergence of a New Discipline. *The International Journal of Digital Curation*, *6*(2). http://www.ijdc.net/article/view/184/251

Higgins, S. (2018). Digital curation: The development of a discipline within information science. *Journal of Documentation*, *74*(6), 1318–1338. https://doi.org/10.1108/JD-02-2018-0024

Humphrey, C. (2006). *E-Science and the Life Cycle of Research*. University of Alberta. https://doi.org/10.7939/R3NR4V

Indolfo, A. C. (2007). Gestão de documentos: Uma renovação epistemológica no universo da arquivologia. *Arquivística.net*, *3*(2), 28–60. https://www.brapci.inf.br/_repositorio/2011/06/pdf_59336b505e_0003553.pdf

ISO. (2008). *ISO/TR 26122:2008 Information and documentation—Work process analysis for records*. https://www.iso.org/standard/43391.html

ISO. (2016). *ISO 15489-1:2016 Information and documentation—Records management—Part 1: Concepts and principles*. https://www.iso.org/standard/62542.html

ISO. (2019). *ISO 30301:2019 Information and documentation—Management systems for records—Requirements*. https://www.iso.org/standard/74292.html

ISO. (2020). *ISO - 01.140.20—Information sciences*. ISO. https://www.iso.org/ics/01.140.20/x/

iso27001security. (2020). *Free ISO27k Toolkit*. ISO27k Toolkit. https://www.iso27001security.com/html/toolkit.html

ISO/IEC. (2013a). *ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO/IEC. (2013b). *ISO/IEC 27002:2013 Information technology—Security techniques: Code of practice for information security management*. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en

ISO/IEC. (2018). *ISO/IEC 27000:2018 Information technology—Security techniques: Information security management systems—Overview and vocabulary*. https://www.iso.org/standard/73906.html

ISO/IEC. (2019). *ISO/IEC 27701:2019 Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines*. https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/16/71670.html

Johnson, C. N. (2016). The benefits of PDCA. *Quality Progress*, *49*(1), 45. https://search.proquest.com/openview/6fb24b731a9c0c8bafd90096fd751e76/1?pq-origsite=gscholar&cbl=34671

Kettinger, W. J., & Li, Y. (2010). The infological equation extended: Towards conceptual clarity in the relationship between data, information and knowledge. *European Journal of Information Systems*, *19*(4), 409–421. https://doi.org/10.1057/ejis.2010.25

Kim, J., Warga, E., & Moen, W. (2013). Competencies Required for Digital Curation: An Analysis of Job Advertisements. *International Journal of Digital Curation*, *8*(1), 66–83. https://doi.org/10.2218/ijdc.v8i1.242

Kowalczyk, S. T. (2017). Modelling the Research Data Lifecycle. *International Journal of Digital Curation*, *12*(2), 331–361. https://doi.org/10.2218/ijdc.v12i2.429

Krogh, G. von., Ichijo, Kazuo., & Nonaka, Ikujiro. (2000). *Enabling knowledge creation: How to unlock the mystery of tacit knowledge and release the power of innovation*. University Press; /z-wcorg/.

Laney, D. (2012). Infonomics: The Practice of Information Economics. *Forbes*. https://www.forbes.com/sites/gartnergroup/2012/05/22/infonomics-the-practice-of-information-economics/

Li, C., & Zhu, Y. (2015). The Challenges of Data Quality and Data Quality Assessment in the Big Data Era. *Data Science Journal*, *14*(2), 1–10. https://datascience.codata.org/articles/10.5334/dsj-2015-002/

Liew, A. (2013). DIKIW: Data, Information, Knowledge, Intelligence, Wisdom and their Interrelationships. *Business Management Dynamics*, *2*(10), 49–62. https://www.researchgate.net/publication/236870996_DIKIW_Data_Information_Knowledge_Intelligence_Wisdom_and_their_Interrelationships

Lillrank, P. (2003). The quality of information. *International Journal of Quality & Reliability Management*, *20*(6), 691–703. https://www.emerald.com/insight/content/doi/10.1108/02656710310482131/full/html

Maceviciute, E., & Wilson, T. (2002). The development of the information management research area. *Information Research: an international electronic journal*, *7*(3). https://paginas.fe.up.pt/~mgi03006/PSI/The%20development%20of%20the%20information%20management%20research%20area.htm

Maciejewski, M., & Gouardères, F. (2019). *Uma Agenda Digital para a Europa | Fichas temáticas sobre a União Europeia | Parlamento Europeu*. Parlamento Europeu. https://www.europarl.europa.eu/factsheets/pt/sheet/64/uma-agenda-digital-para-a-europa

Marconi, M. de A., & Lakatos, E. M. (2003). *Fundamentos de metodologia científica.* (5.ª ed.). Atlas.

Mathews, L. (2019). A Ransomware Attack Knocked The Weather Channel Off The Air. *Forbes*. https://www.forbes.com/sites/leemathews/2019/04/19/a-ransomware-attack-knocked-the-weather-channel-off-the-air/#2a7ff1c179c9

McLean, R. (2019). Capital One data breach: A hacker gained access to 100 million credit card applications and accounts—CNN. *CNN Business*. https://edition.cnn.com/2019/07/29/business/capital-one-data-breach/index.html

Mestrado em Gestão e Curadoria de Informação | NOVA Guia de Cursos. (2020). Universidade Nova de Lisboa. https://guia.unl.pt/pt/2019/fcsh/program/4359#structure

Moen, R., & Norman, C. (2006). *Evolution of the PDCA cycle*. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.470.5465&rep=rep1&type=pdf

Moxey, M. (2019). Tourism ministry's servers breached. *EyeWitness News*. https://ewnews.com/tourism-ministrys-servers-breached

Newman, L. H. (2019). The Biggest Cybersecurity Crises of 2019 So Far. *Wired*. https://www.wired.com/story/biggest-cybersecurity-crises-2019-so-far/

Nonaka, I., & Takeuchi, Hirotaka. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press; /z-wcorg/.

Ochôa, P. (2017). Painel «Perfis e competências profissionais». *Encontro Curadoria Digital – Estratégias e experiências: atas*, 62–65. https://repositorio.ual.pt/bitstream/11144/3708/3/Ebook%20Encontro%20Curadoria%20Digital%200509.pdf

Ochôa, P., & Pinto, L. G. (2017). Transformação digital e competências digitais: Estratégias de gestão e literacia. *Literacia, Media e Cidadania - Livro de Atas do 4.º Congresso*, *1*, 386–398. http://www.lasics.uminho.pt/ojs/index.php/cecs_ebooks/article/view/2689

Pennock, M. (2007). Digital Curation: A Life-Cycle Approach to Managing and Preserving Usable Digital Information. *Library & Archives*, *1*(1), 1–3. http://www.ukoln.ac.uk/ukoln/staff/m.pennock/publications/docs/lib-arch_curation.pdf

Pinto, L. G., & Ochôa, P. (2006). *A imagem das competências dos profissionais de informação-documentação*.

Polanyi, M. (1966). *The tacit dimension*. Doubleday.

Poole, A. H. (2013). Now is the Future Now? The Urgency of Digital Curation in the Digital Humanities. *Digital Humanities Quarterly*, *7*(2). http://www.digitalhumanities.org/dhq/vol/7/2/000163/000163.html

Pouchard, L. (2015). Revisiting the Data Lifecycle with Big Data Curation. *International Journal of Digital Curation*, *10*. https://doi.org/10.2218/ijdc.v10i2.342

Priberam. (2008a). Eficácia. Em *Dicionário Priberam da Língua Portuguesa*. https://dicionario.priberam.org/efic%C3%A1cia

Priberam. (2008b). Eficiência. Em *Dicionário Priberam da Língua Portuguesa*. https://dicionario.priberam.org/efici%C3%AAncia

Ransomware. (2020). Em *Wikipédia, a enciclopédia livre*. https://pt.wikipedia.org/w/index.php?title=Ransomware&oldid=57658497

Reyes, A., Barreto, C., Cerdeirinha, J., Guedes, M. de S., Teixeira, P., & Néo, S. (2017). Gestor e curador da informação: Tendências, perfis e estratégias de

reconhecimento. *Páginas a&b.*, *3*(7), 3–15. https://doi.org/10.21747/21836671/pag7a1

Ruesta, C. B. (2012). *Série ISO 30300: Sistema de gestão para documentos de arquivo*. BAD. https://www.bad.pt/publicacoes/Serie_ISO_30300.pdf

Sajko, M., Rabuzin, K., & Bača, M. (2006). How to calculate information value for effective security risk assessment. *Journal of Information and Organizational Sciences*, *30*(2), 263–278. https://www.researchgate.net/publication/26596362_How_to_calculate_information_value_for_effective_security_risk_assessment

Santos, V. dos, & Candeloro, R. J. (2006). *Trabalhos acadêmicos: Uma orientação para a pesquisa e normas técnicas.* Age.

Saracevic, T. (2010). Information science. Em *Encyclopedia of Library and Information Sciences* (3.ª ed., p. 2570 — 2585). Taylor & Francis.

Sayão, L. F., & Sales, L. F. (2012). Curadoria digital: Um novo patamar para preservação de dados digitais de pesquisa. *Informação e Sociedade*, *22*(3), 179–191. https://periodicos.ufpb.br/ojs2/index.php/ies/article/view/12224

Shannon, C. E. (1948). A mathematical theory of communication. *The Bell System Technical Journal*, *27*, 379–423. http://www.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

Silva, G. C., Fernandes, M., & Aleixo, M. R. (2019). Comportamento informacional e literacia digital: Uma experiência pedagógica. *Literacia, Media e Cidadania – Livro de Atas do 5.º congresso*, 424–436.

Sokovic, M., Pavletic, D., & Pipan, K. K. (2010). Quality improvement methodologies–PDCA cycle, RADAR matrix, DMAIC and DFSS. *Journal of achievements in*

materials and manufacturing engineering, *43*(1), 476–483. http://jamme.acmsse.h2.pl/papers_vol43_1/43155.pdf

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. *2018 International Conference on Information Systems and Computer Science (INCISCOS)*, 294–300. https://doi.org/10.1109/INCISCOS.2018.00049

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Cybercrime in the Digital Economy*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Wang, Y., & Wong, A. K. C. (2003). From association to classification: Inference using weight of evidence. *IEEE Transactions on Knowledge and data engineering*, *15*(3), 764–767. https://ieeexplore.ieee.org/document/823353

Weber, M. (1947). *The theory of social and economic organization* (T. Parsons, Ed.). Oxford University Press.

Werthein, J. (2000). A sociedade da informação e seus desafios. *Ciência da Informação*, *29*(2), 71–77. http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf

Whitman, M. E., & Mattord, H. J. (2016). *Principles of information security* (5.ª ed.). Cengage Learning.

Why and How to Value Your Information as an Asset. (2015). Gartner.Com. //www.gartner.com/smarterwithgartner/why-and-how-to-value-your-information-as-an-asset/

Wilson, T. D. (2003). Information Management. Em J. Feather & P. Sturges, *International Encyclopedia of Information and Library Science* (2.ª ed.).

Winter, L. A. C., & Botelho, M. M. (2014). Lei de informação privilegiada: Uma análise jurídico-econômica. *Direito e Economia I: XXIII Congresso Nacional do CONPEDI*, 133–147. http://publicadireito.com.br/artigos/?cod=109a44b224f37495

Yang, S.-C., & Farn, C.-K. (2009). Social capital, behavioural control, and tacit knowledge sharing—A multi-informant design. *International Journal of Information Management*, *29*(3), 210–218. https://doi.org/10.1016/j.ijinfomgt.2008.09.002

Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *JASIST*, *58*(4), 479–493. https://doi.org/10.1002/asi.20508